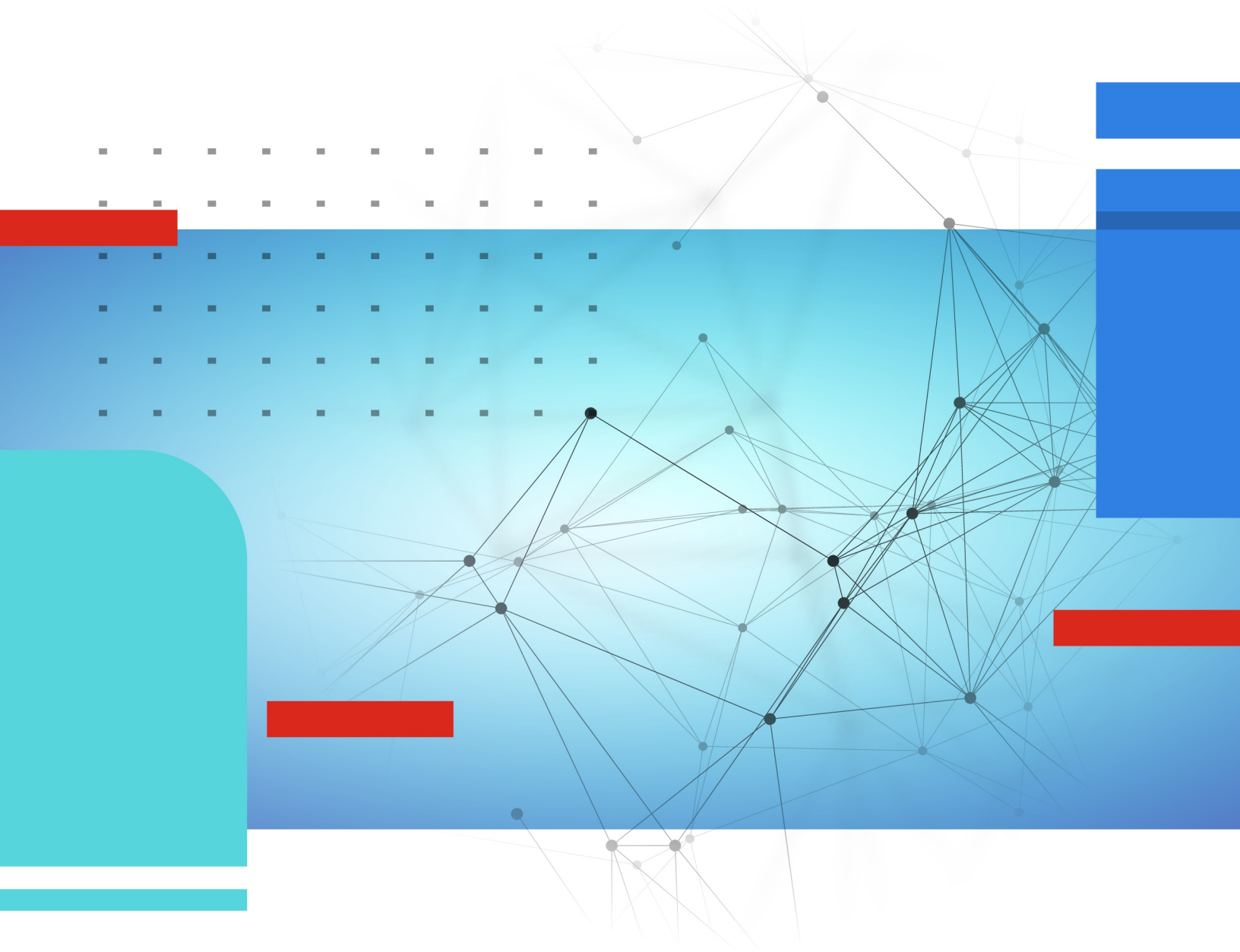
Administration Guide

FortiSASE 24.2.63



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

August 06, 2024
FortiSASE 24.2.63 Administration Guide
72-24263-1028428-20240806

TABLE OF CONTENTS

Change log

Date	Change description
2024-07-19	Initial release of 24.2.63.
2024-07-23	Updated: • Network restrictions on page 89 • Configuring FortiSASE with Entra ID SSO in FortiClient agent-based mode on page 211 • Connection on page 246 • Settings on page 255
2024-07-26	Updated: • FortiCloud account prerequisites on page 67 • Connection on page 246 • Settings on page 255
2024-08-06	Updated: • FortiFlex licensing on page 19 • Entra ID domains on page 263

Getting started

FortiSASE is a software-as-a-cloud-delivered service that allows clients to securely access the internet with the protection from FortiOS. With FortiSASE, you can ensure to protect remote off-net endpoints and users 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 users.

FortiSASE works with various FortiCloud services in the background to deliver a seamless service for securing your internet access.

In terms of security, FortiSASE offers the following features to protect clients:

- Antivirus
- Web Filter
- Intrusion prevention
- File filter
- Data loss prevention
- Application control
- SSL inspection

Use the following resources to get started with FortiSASE:

Task	Documentation links
Review FortiSASE requirements	See Requirements on page 9.
Review FortiSASE licensing	See Licensing on page 10.
Get started with initializing FortiSASE	See Initializing FortiSASE on page 11.
Get started with securing FortiSASE remote users	See: • Policies on page 139 • Security on page 145 • Endpoints on page 244
Learn about new FortiSASE features	See What's new.
Learn about best practices for deploying a FortiSASE architecture	Go to Best Practices | 4-D resources. Review the document categories.
Review information about FortiSASE releases, including resolved and known issues	See FortiSASE Release Notes.

Requirements

The following items are required before you can initialize FortiSASE:

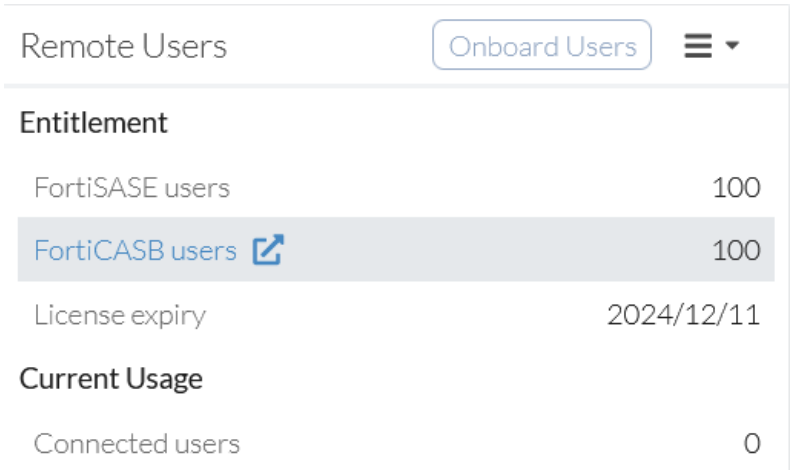
Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Launching FortiSASE requires a primary FortiCloud account. A primary FortiCloud account can invite other users to launch FortiSASE as secondary users.
Internet access	You must have internet access to create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

You can only create one FortiSASE instance per FortiCloud account.

Licensing

The FortiSASE portal enforces license requirements when you log in. FortiSASE requires the FortiSASE subscription based on the number of remote users. Some FortiSASE features, such as assisted onboarding, require the Advanced or Comprehensive license. See the SASE and Zero Trust Ordering Guide and Product integration and support for licensing details.

To check the current license entitlement for remote users, go to *Dashboards* > *Status* and observe this information in the *Remote Users* widget.



From the screenshot, you can determine the following information:

- *Entitlement* > *FortiSASE users*: 100
- *Current Usage* > *Connected users*: 0
- Number of FortiSASE users available: 100

The FortiSASE header in the top-left of the portal also reflects license type. An instance with the Advanced or Comprehensive license has a modified header with a matching label.

For example, for an instance with an Advanced license, the following header displays:

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.

During initial provisioning, you can select fewer security sites than the maximum you are entitled to. In this case, upon each login, the FortiSASE portal prompts you to select up to the maximum number of security sites.

If you decide to add additional security sites using this prompt, then FortiSASE allows for increasing the number of security sites without FortiCare Support. FortiSASE may experience up to 10 minutes of downtime when the entitlement is applied. If any errors occur, FortiSASE cannot automatically rollback without FortiCare Support.

For provisioning, you must select a minimum of two security sites for redundancy.

Do one of the following:

- Select up to the maximum number of entitled security sites and click *Apply Now*.
- Simply click *Apply Later* to acknowledge this prompt. It appears upon the next login.

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 desired email. FortiSASE sends instructions and an invitation code to this email address. The user uses this code to connect FortiClient to FortiSASE.
   e. If desired, enable and configure *Temporary administrative password*. 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 on page 198.

Introduction

FortiSASE is a software-as-a-cloud-delivered service that allows clients to securely access the internet with the protection from FortiOS. With FortiSASE, you can ensure to protect remote off-net endpoints and users 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 users.

FortiSASE works with various FortiCloud services in the background to deliver a seamless service for securing your internet access.

In terms of security, FortiSASE offers the following features to protect clients:

- Antivirus
- Web Filter
- Intrusion prevention
- File filter
- Data loss prevention
- Application control
- SSL inspection

Security features are customizable and offer many familiar settings as you would see on a FortiGate.

Following are examples of common FortiSASE use cases:

FortiSASE component	Use case	Description
Secure internet access (SIA)	Agent-based remote user internet access	Secure access to the internet using FortiClient agent
	Agentless remote user internet access	Secure access to the internet using FortiSASE secure web gateway (SWG)
	Site-based remote user internet access using FortiExtender	Secure access to the internet using FortiExtender device as FortiSASE LAN extension
	Site-based remote user internet access using FortiAP	Secure access to the internet using FortiAP edge device that FortiSASE manages

FortiSASE component	Use case	Description
Secure private access (SPA)	Zero trust network access (ZTNA) private access	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases. This access method allows for a direct (shortest) path to private resources.
	SD-WAN private access	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network. This access method extends private access for TCP- and UDP-based applications and offers data center redundancy.
	Next generation firewall (NGFW) private access	Access to private company-hosted applications behind the FortiGate NGFW. This use case extends private access for UDP-based applications and agentless remote users.
Secure SaaS access	FortiCASB SaaS access	Access to SaaS applications using FortiCASB Cloud/API
	FortiSASE Inline-CASB	Access control to SaaS applications using FortiSASE inline-CASB and SSL deep inspection on endpoint
SIA and SPA	Site-based remote users using FortiGate SD-WAN as a secure edge	Secure access to the internet using FortiGate as FortiSASE LAN extension

For details on these FortiSASE use cases, see the 4-D FortiSASE Architecture Guide.

For details on the deployment process, see FortiSASE Cloud Deployment.

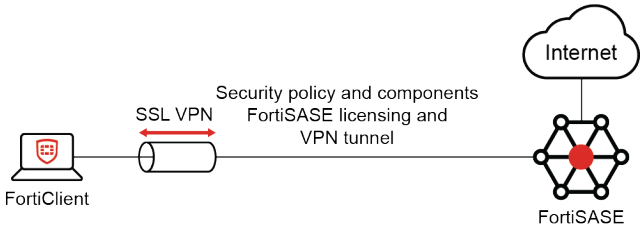
User provisioning is made simple, whether you are creating local users in bulk, integrating users from your Active Directory or LDAP server, or integrating with SAML authentication. You can also easily group your users to apply similar VPN or SWG policies.

See Service Organization Controls (SOC2) compliance standard.

FortiClient agent-based mode using FortiClient

In FortiClient agent-based mode, endpoints connect to a FortiSASE VPN tunnel to secure their traffic. Once provisioned, clients are connected through an always-up VPN connection to ensure FortiSASE scans traffic to the internet.

This mode requires FortiSASE user-based licensing. See the SASE and Zero Trust Ordering Guide.



The provisioning process for this mode is as follows:

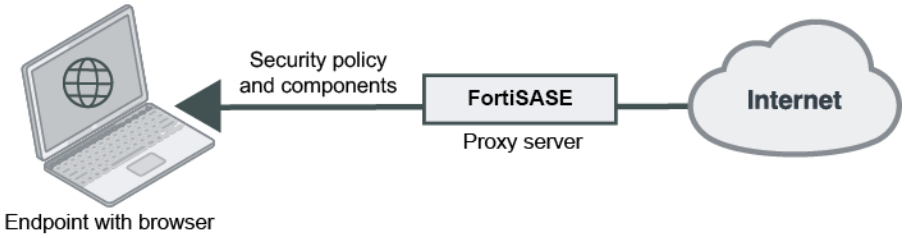
1. The administrator initializes the FortiSASE environment.
2. The administrator configures policies and security components in FortiSASE as desired, including configuring the desired policies. See Adding policies to perform granular firewall actions and inspection on page 139.
3. The administrator provisions end users on FortiSASE and emails invitations to them. FortiSASE supports remote authentication methods such as LDAP. See Authentication Sources and Access on page 198 for descriptions of the provisioning process for different authentication methods.
4. Download FortiClient to endpoints and connect to FortiClient Cloud using the code included in the invitation email. This can be completed by the administrator when preprovisioning endpoints before distributing to end users, or by the end users themselves.
5. FortiClient connects to FortiClient Cloud to activate its FortiSASE license and provision the FortiSASE VPN tunnel.
6. End users connect to the FortiSASE tunnel to secure their traffic.
7. FortiSASE applies the appropriate policies to endpoints.
8. The administrator can view logs in FortiSASE and modify the configuration as desired. See Logging on page 274.

This mode also supports configuring Zero Trust Network Access (ZTNA). In this deployment configuration, FortiSASE joins the Fortinet Security Fabric to share endpoint information with the FortiGate, allowing a corporate FortiGate to implement ZTNA for remote users who are already registered to FortiSASE. See the *FortiSASE ZTNA Deployment Guide* for details.

SWG agentless mode

In secure web gateway (SWG) agentless mode (formerly known as SWG mode), users configure FortiSASE as a SWG server on their device at the OS level or in a browser. Once configured, the SWG policies configured in FortiSASE protect sessions initiated in browsers.

This mode requires FortiSASE user-based licensing. See the FortiSASE Ordering Guide.



The provisioning process for this mode is as follows:

1. The administrator initializes the FortiSASE environment.
2. The administrator configures policies and security components in FortiSASE as desired, including enabling SWG and configuring the desired SWG policies. See Configuring a SWG policy on page 143.
3. The administrator configures end users on FortiSASE and distributes the SWG server information to them.
4. End users configure their OS or browser to use the FortiSASE SWG server. When the browser displays an authentication prompt, the end user enters their FortiSASE user credentials.
5. FortiSASE applies the appropriate policies to sessions initiated in the browser.
6. The administrator can view logs in FortiSASE and modify the configuration as desired. See Logging on page 274.

Dedicated public IP addresses

The Public IP Deployment Guide provides use cases, licenses required, and deployment details.

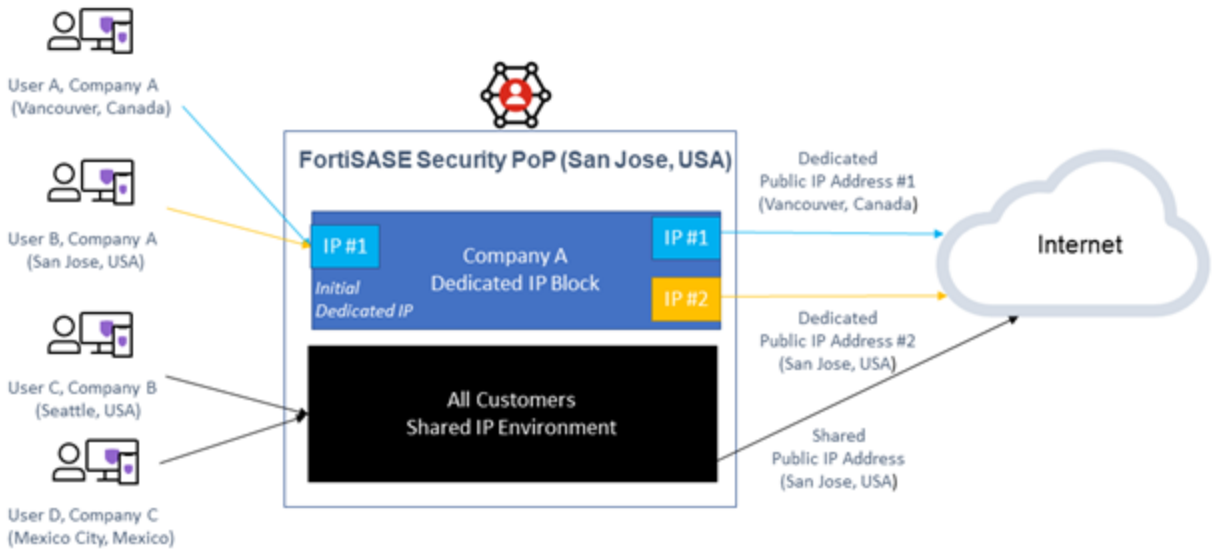
The FortiSASE default shared IP address environment presents some problems for customers and their remote users:

- Since the same public IP address is used for all outgoing traffic, identification and isolation of each specific customer's remote user traffic is not possible.
- Since the public IP address used for outgoing traffic belongs to an IP address block in the same geographical location as the security point of presence (PoP) or region that users are connected to, their content is limited to that specific location when accessing services relying on geolocation.

Using dedicated public IP addresses for each customer's remote user traffic and public IP addresses that are mapped to a specified country can solve these problems.

The network diagram illustrates some benefits of using FortiSASE dedicated public IP addresses as this section further describes:

- Traffic identification and isolation for IP reputation control
- Geolocation rules
- Source IP anchoring



Implementing dedicated public IP addresses is currently impactful to the operation of the FortiSASE instance. FortiSASE Operations recommends that a request to implement dedicated public IP use cases be raised with ample time in advance before onboarding any remote users or implementing features such as FortiAP, FortiExtender, or FortiGate edge device support to avoid service disruption.

The number of security PoPs that are accessible by remote users depends on the FortiSASE license tier and number of users. See Number of security data centers accessible per license on page 325.

Currently, you must manually configure the dedicated public IP use cases for FortiSASE on the backend. See frequently answered questions for Dedicated public IP addresses

Embedded onboarding guide

An embedded onboarding guide for FortiSASE displays upon first login. You can also display it later if you skip it. This guide contains instructions and videos embedded into the FortiSASE portal that streamline initial configurations for the secure internet access (SIA) endpoint use case. This use case provides remote users with secure access to the internet using the FortiClient agent. See SIA for agent-based remote users.

Access to the embedded onboarding guide in your FortiSASE instance requires an Advanced remote users FortiSASElicense or a Comprehensive remote users FortiSASE license. See the SASE and Zero Trust Ordering Guide.

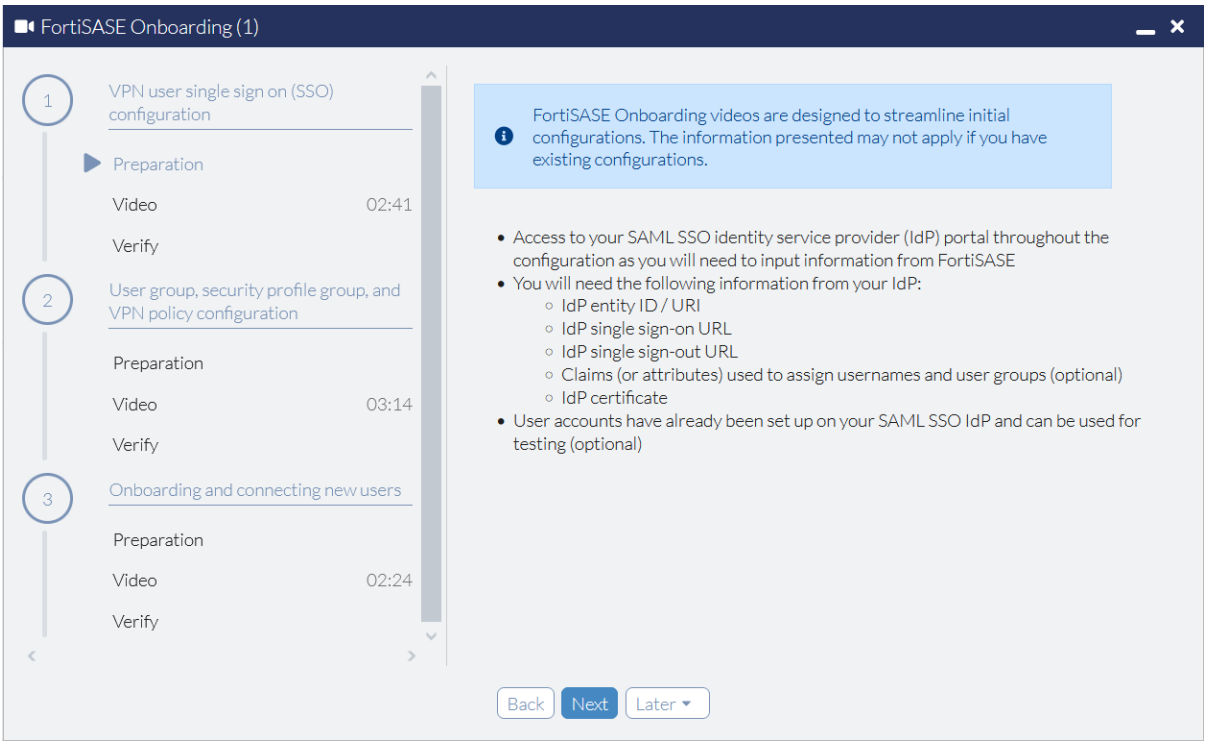
The information presented may not apply to instances with existing configurations.

The onboarding guide focuses on these configuration topics:

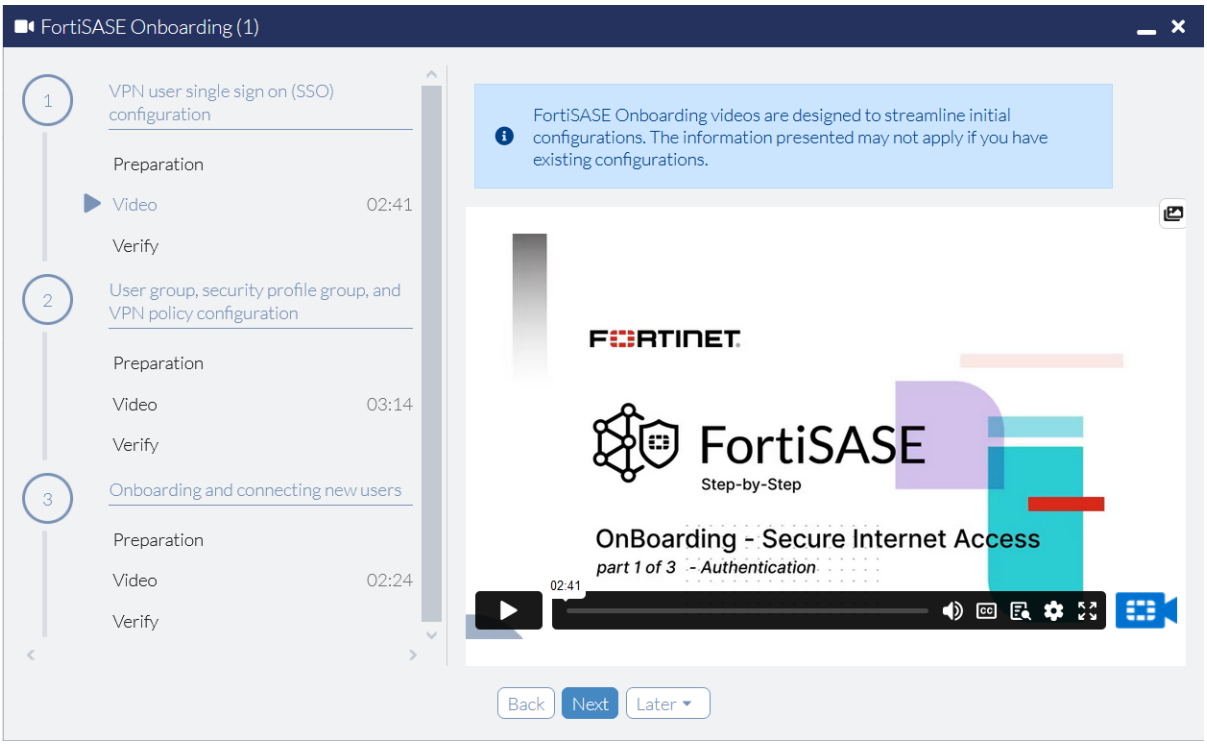
- VPN user single sign-on configuration
- User group, security profile group, and VPN policy configuration
- Onboarding and connecting new users

The guide breaks down each topic into the following sections:

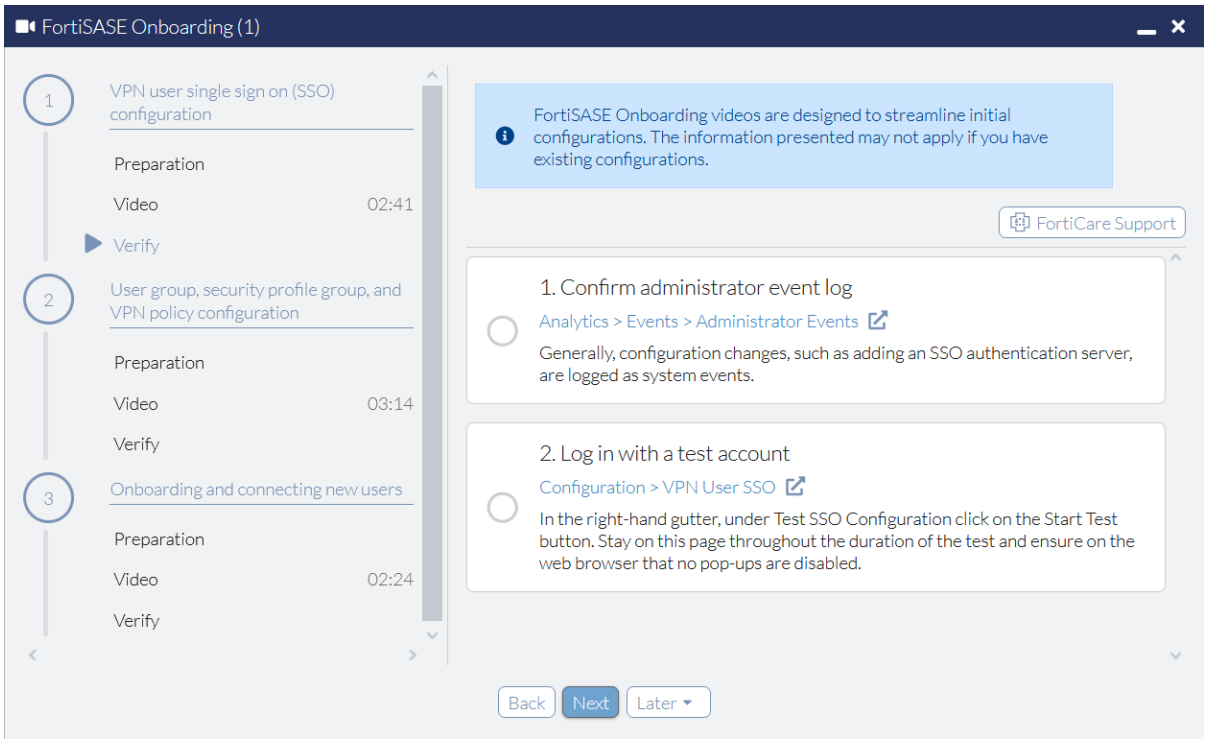
- **Preparation**: steps that you must perform before starting the configuration topic.



- **Video**: brief video that demonstrates the steps that you must perform to complete the configuration or task.



- **Verify**: checklist of steps to perform to ensure that you have configured the FortiSASE settings correctly.

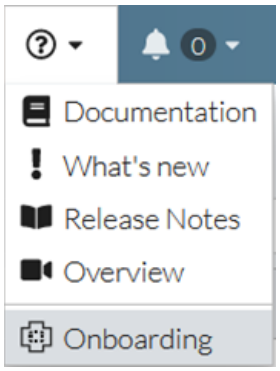


  - To go to the corresponding FortiSASE portal page to perform the verification step, click the link provided.
  - Click the checkbox input next to the verification step to mark it as completed.
  - If you require technical assistance, click *FortiCare Support* to open the Fortinet Support site.

You can go back and forth between sections and topics by clicking the sections in the left pane or by using the *Back* and *Next* buttons, as desired.

Typically, after the *Video* section, you can minimize the guide and perform the configuration settings in the FortiSASE portal as the video demonstrates. You can resume or maximize the guide by clicking the onboarding title at the bottom of the screen.

If you click *Later* or *Skip onboarding* to skip the onboarding for now, you can access the guide later from the Help dropdown in the app header by clicking *Onboarding*.



FortiFlex licensing

FortiSASE supports applying FortiFlex entitlements generated from within the FortiFlex portal to your instances. You must apply the appropriate FortiFlex Program and Point Pack SKUs for access to the FortiFlex portal from within your FortiCloud account. See the FortiFlex Program Ordering Guide.

Before adding a Flex entitlement for FortiSASE from within the FortiFlex portal, ensure that your FortiCloud account does not have any existing FortiClient EMS Cloud or FortiSASE entitlements. Otherwise, you will not be able to add a new Flex entitlement for FortiSASE.

FortiSASE entitlements created in the FortiFlex portal must be active for at least 90 days.

For details on supported FortiFlex FortiSASE service offerings and FortiFlex deployment steps, see Service Offerings and Deploying FortiFlex.

Required services and ports

The following summarizes ports that FortiSASE uses. In addition to those in the table, FortiSASE also uses ICMP.

Usage	Protocol	Port
SSL VPN portal	TCP	443
DTLS VPN	UDP	
IPsec VPN IKE		500
IPsec NAT-T		4500
CAPWAP		5246
SAML authentication	TCP	7831
Web Filter		8008 8010 8015 8020
Customer-specific secure web gateway port assignment		10445-50445

Signing in as an IAM user

You can log in to FortiSASE as an Identity & Access Management (IAM) user. You must first create an IAM user by following the steps in To create an IAM user with the wizard:. When configuring the IAM user, ensure that you add FortiSASE to the services that the user can access.

You should use IAM instead of FortiCloud subaccounts in cases where multiple users access the FortiSASE customer portal.

To sign in as an IAM user:

1. Go to the FortiSASE portal.
2. Click *SSO Login*.
3. Click *IAM Login*.
4. Log in with the user credentials from the CSV that you downloaded when creating the IAM user in To create an IAM user with the wizard.

System status notifications

By default, the FortiSASE primary account holder is automatically subscribed to FortiSASE system status email notifications from https://status.fortisase.com.

To manually subscribe to FortiSASE system status notifications via email and other notification types including SMS, Slack, webhooks, Atom feeds, and RSS feeds for yourself and secondary administrators, go to https://status.fortisase.com and click *Subscribe to updates*.

When subscribed to FortiSASE system status notifications, you receive email notifications whenever FortiSASE Operations creates, updates, or resolves an incident.

Select availability features

FortiSASE includes several features with select availability, which are features that are released but are not available by default for all customers. Following is a table that describes some of these features and the associated conditions when they are enabled on existing FortiSASE instances.

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
Network restrictions removed on page 23	Support for removing network restrictions for customer networks.	Yes	Yes	When enabling this feature, FortiSASE service may be unavailable for brief periods of time. Completing the process requires up to a two-hour scheduled maintenance window.
Remote VPN user identification on page 24	Support unique remote VPN IP address ranges per FortiSASE security PoP within the overall 100.65.0.0/16 range. Remove source NAT (SNAT) for remote VPN user traffic destined for secure private access hubs.	No	Yes	When enabling this feature, data loss may be possible. Resetting your FortiSASE instance to default may be required. If your FortiSASE instance requires a reset, then the following next steps are required to resume normal operation: • Manual setting reconfiguration • Scheduled maintenance window to re-onboard remote users

Select availability feature	Description	Enabled for new instances	Can be enabled for existing instances*	Associated conditions when enabled
SD-WAN On-Ramp support on page 24	Support an IPsec tunnel connection between a certified IPsec device and a FortiSASE SD-WAN On-Ramp location. This support requires a separate FortiSASE subscription license per certified IPsec device.	No	Yes	No associated conditions when enabled.
Supporting external IdP users on page 25	External IdP users can log into FortiSASE with their company-provided user credentials using a third-party SAML IdP	No	Yes, limited beta in FortiCloud	Involves a transition period from using FortiCloud Identity & Access Management users to using external IdP users.

* A customer can request enabling a select availability feature for an existing FortiSASE instance by creating a new ticket with FortiCare Support.

Network restrictions removed

FortiSASE includes support for removing network restrictions.

The following networks are available for your network configuration:

- 10.8.0.0/16
- 10.16.0.0/16
- 100.64.0.0/10 (except 100.65.0.0/16)
- 172.16.0.0/12
- 192.168.0.0/16

For new FortiSASE instances, support for removing network restrictions is enabled by default. For existing FortiSASE instances, you must request support for removing network restrictions by creating a new FortiCare ticket.

With the requested network restrictions removed, FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and you have configured the SPA hub in FortiSASE with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses LDAP servers with *AD Users & Groups* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs with *Access Type* set to *Public* in the LDAP server settings and may require some configuration or topology changes.

Remote VPN user identification

FortiSASE allows administrators to identify remote VPN users uniquely in internet and private access traffic logs, which you can achieve by enabling these capabilities:

- Adding support for unique remote VPN IP address ranges per FortiSASE security PoP within the overall 100.65.0.0/16 range. Previously, remote VPN IP address ranges were not unique between security PoPs.
- Removing source NAT (SNAT) for remote VPN user traffic destined for secure private access hubs. By default, FortiSASE performs SNAT for such traffic.

For a new FortiSASE instance, this select availability feature is disabled by default. To add support for this select availability feature to your FortiSASE instance, create a new ticket with FortiCare Support.

As a select availability feature, if you enable this feature, the following is possible with your FortiSASE instance:

- Data loss
- Resetting the instance may be required.

If your FortiSASE instance requires a reset, then the following next steps are required to resume normal operation:

- Manual setting reconfiguration
- Scheduled maintenance window to re-onboard remote users

SD-WAN On-Ramp support

SD-WAN On-Ramp is a select availability feature that requires a FortiSASE instance with an Advanced or a Comprehensive license applied and a separate FortiSASE subscription license per certified IPsec device. This license restricts the number of On-Ramp locations that you can deploy based on the number of seats (two to eight seats) that the license specifies. Contact your Fortinet sales/partner representative to purchase a FortiSASE subscription license for each certified IPsec device.

The FortiGate is the only certified IPsec device that can be used for SD-WAN On-Ramp.

You can configure a certified IPsec device for SD-WAN On-Ramp by setting up an IPsec tunnel between the certified IPsec device and a FortiSASE SD-WAN On-Ramp location. See SD-WAN On-Ramp on page 65.

SD-WAN On-Ramp support is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Supporting external IdP users

External identity provider (IdP) users can log into FortiSASE with their company-provided user credentials using a third-party SAML IdP.

External IdP support is a limited beta feature in FortiCloud and a select availability feature in FortiSASE that is not enabled by default on new instances. If you require external IdP support for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

For information on managing external IdP roles and users for cloud products, see External IdP roles.

Dashboards

FortiSASE includes dashboards so you can easily monitor device inventory, security threats, traffic, and network health. FortiSASE includes the following default dashboards:

Dashboard	Description
Status	Provides an overview of your current FortiSASE environment and endpoint status.
Asset Map	Displays the geographical location of assets, including servers, on a global map. Also indicates which server has logging enabled.
FortiView	Comprehensive monitoring system for your network that integrates real-time and historical data into a single view. You can use it to log and monitor threats to networks, filter data on multiple levels, and keep track of administrative activity.

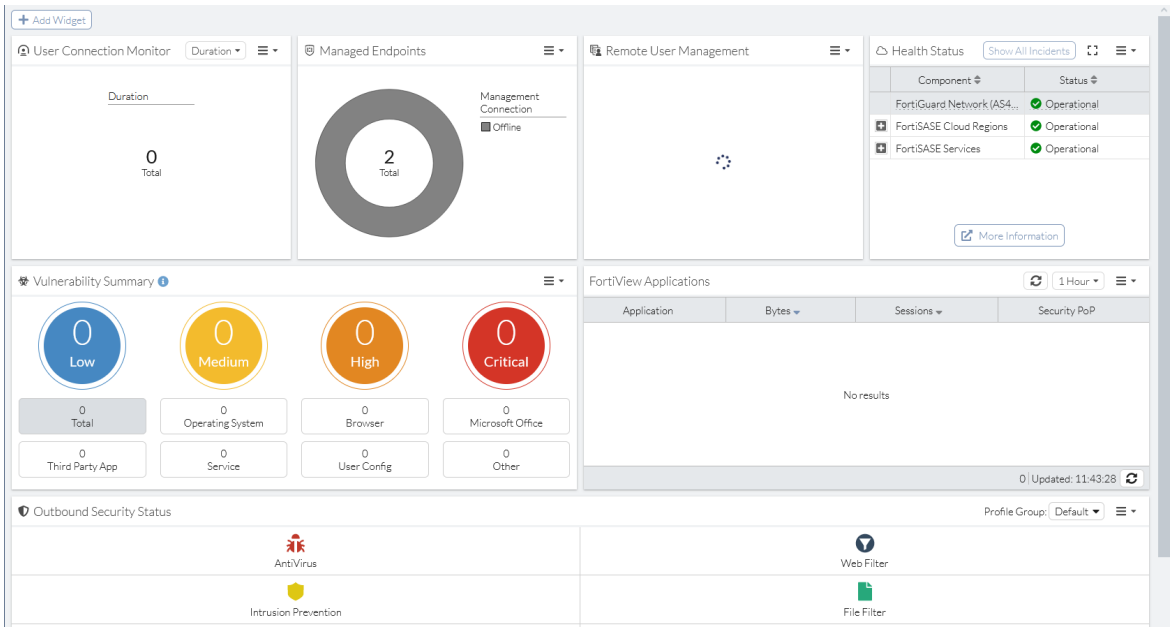
Adding a custom dashboard

You can create and modify a dashboard of a customizable widget array.

To add a custom dashboard:

1. Under *Dashboards*, click +.
2. In *Add Dashboard*, enter the desired name. Click *OK*.
3. The blank dashboard displays. Click *Add Widget*.
4. In the *Add Dashboard Widget* pane, select the desired widget to add to the dashboard. Repeat to add all desired widgets.
5. You can further customize the dashboard by moving and resizing widgets. To move a widget, hover over the widget title, then click and drag the widget to the desired location. To resize the widget, from the menu in the upper right corner of the widget, select *Resize*, and select the desired number of spaces for the widget to occupy. The following

shows a custom dashboard that differs from the default status and security dashboards:

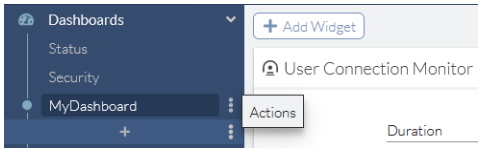


Resetting all dashboards

You can reset all dashboards. This deletes all custom dashboards from FortiSASE and resets the Status and Security dashboards to their default configurations. If you deleted a default dashboard, the reset restores it.

To reset all dashboards:

1. Click the *Actions* icon beside the + button under *Dashboards*.



2. Select *Reset all Dashboards*.
3. In the confirmation message, click *OK*.

Drilling down on vulnerabilities

You can drill down on vulnerabilities on the Security dashboard.

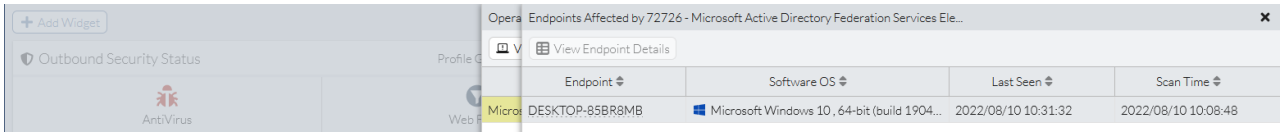
To drill down on vulnerabilities that belong to the same category:

1. Go to *Dashboards* > *Security*.
2. In the *Vulnerability Summary* widget, click the desired category, such as *Operating System*. FortiSASE displays a pane that shows all endpoints that have operating system vulnerabilities.

To drill down to view all endpoints affected by certain vulnerabilities:

1. Go to *Dashboards* > *Security*.
2. In the *Vulnerability Summary* widget, click the desired category, such as *Operating System*, or risk level, such as *Medium*.
3. FortiSASE displays a pane that shows all endpoints that have the applicable vulnerabilities. To view endpoints that a specific vulnerability affects, do one of the following:
   - Click the desired vulnerability, then click *View Affected Endpoints*.
   - Right-click the endpoint, then click *View Affected Endpoints*.

   FortiSASE displays information for all endpoints that vulnerability affects.



FortiView monitors

The following FortiView monitors are available in FortiSASE:

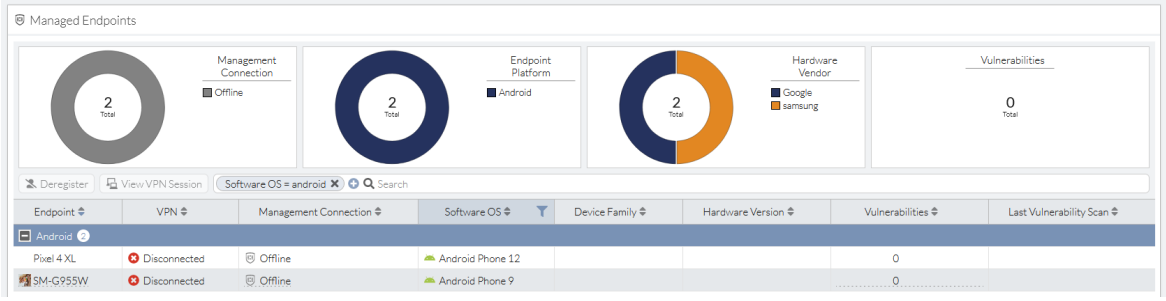
Dashboard	Displays...
Sources	Sources by traffic volume and drilldown by source.
Thin-Edge	Thin-Edge devices by traffic volume and drilldown by Thin Edge device.
Destinations	Destinations by traffic volume and drilldown by destination.
Applications	Applications by traffic volume and drilldown by application.
Cloud Applications	Cloud applications and drilldown by application.
Web Sites	Websites by session count and drilldown by domain.
Policies	Policies by traffic volume and drilldown by policy number.
Sessions	Sessions by traffic source.
VPN	VPN connections by user.
Threats	Threats and drilldown by threat.

Adding a custom monitor

You can create and modify a custom monitor. For example, consider that you want to create a monitor to monitor all managed Android endpoints. You can create a custom monitor based on the Managed Endpoints monitor, and apply a filter to display only Android endpoints. You can simply view this custom monitor whenever you want to monitor your Android endpoints.

To add a custom monitor:

1. Under *Dashboards* > *MONITOR*, click +.
2. In *Add Monitor*, select the desired FortiView or status monitor. The example selects *Managed Endpoints*.
3. In the *Name* field, enter the desired name. Click *OK*. You can further customize the monitor by applying filters or configuring the sort order on columns as desired. The example has a filter applied to display only Android endpoints.

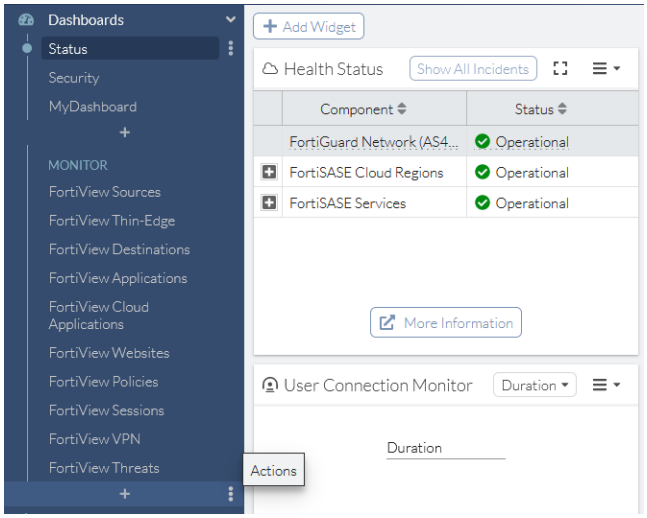


Resetting all monitors

You can reset all monitors. This deletes all custom monitors from FortiSASE and resets the default monitors to their default configurations. If you deleted a default monitor, the reset restores it.

To reset all dashboards:

1. Click the *Actions* icon beside the + button under *Dashboards* > *MONITOR*.



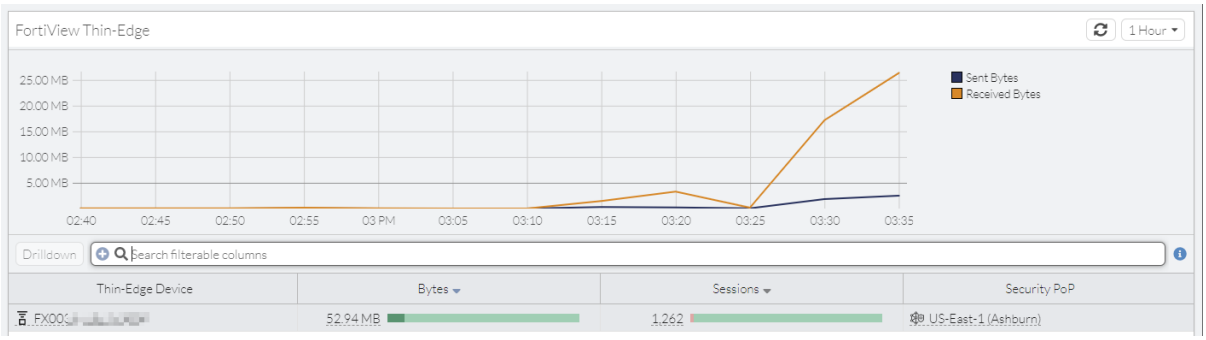
2. Select *Reset all Monitors*.
3. In the confirmation, click *OK*.

Monitoring thin-edge bandwidth usage

You can view FortiExtender devices' bandwidth usage from the FortiView Thin-Edge monitor.

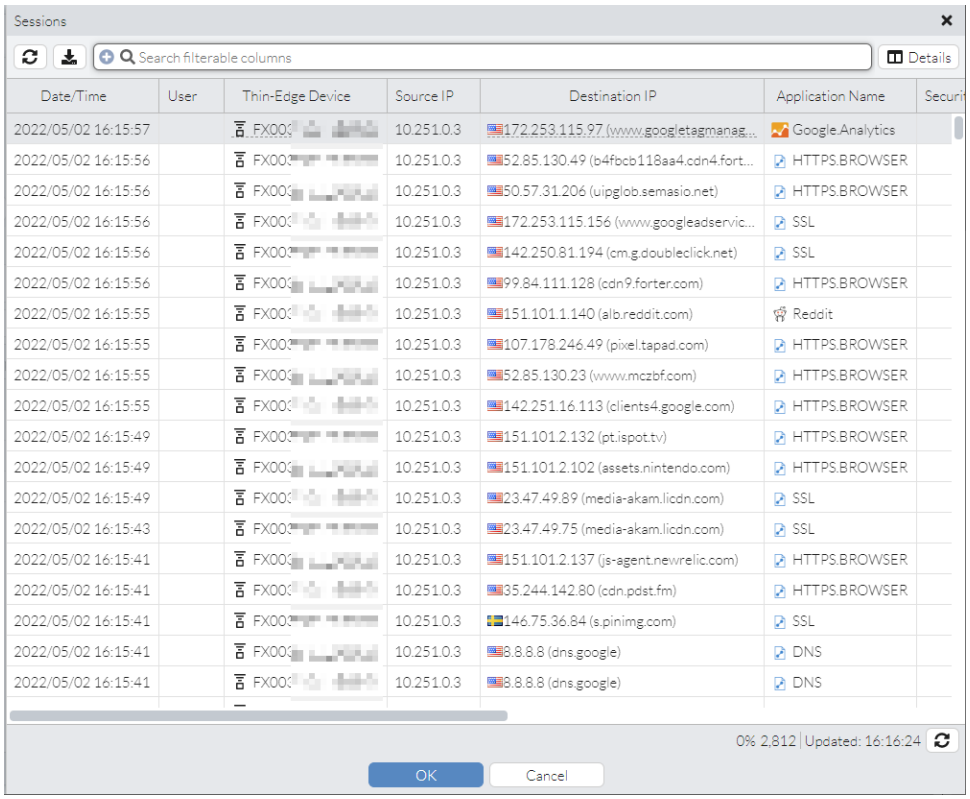
To drill down on thin-edge bandwith usage data:

1. Go to *Dashboards* > *MONITOR* > *FortiView Thin-Edge*.



2. Select the desired FortiExtender.
3. Click *Drilldown*.
4. Go to the *Source*, *Destinations*, *Applications*, *Web Sites*, and *Policies* tabs to view the respective traffic.

5. Click *View Sessions* to view sessions associated with the selected tab.



Thin-Edge

You can view thin-edge devices through the corresponding status widget, which displays online status, security PoP locations, and entitlements through corresponding dropdown menus.

To view FortiExtender entitlements:

1. Go to *Dashboards* > *Status* and in the *Thin-Edge* widget, click on the *Entitlements* dropdown menu. If this widget does not exist, add a new *Thin-Edge* widget. See Adding a custom dashboard on page 26.

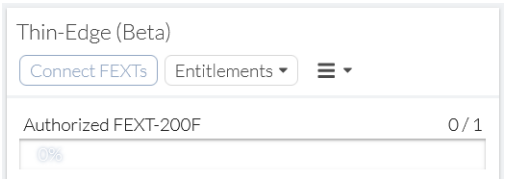
The *Entitlements* dropdown menu is only available if you have applied at least one FortiSASE ThinEdge license to a FortiExtender device.

The FortiExtender-200F is the only supported model and *Entitlements* only shows authorized status and entitlement counts for this model.

2. Within the *Entitlements* view, view the following statuses:

- Number of authorized FortiExtender devices
- Total number of entitlements

In the following screenshot, the *Thin-Edge* widget's *Entitlements* view displays zero authorized FortiExtender devices and one registered thin-edge management entitlement. In this case, FortiSASE can manage only one FortiExtender device.



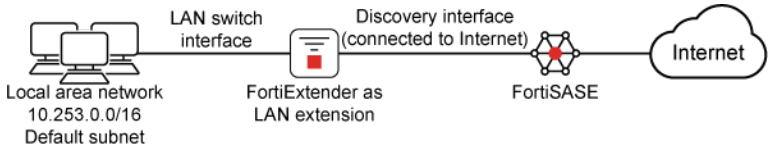
Edge devices

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

FortiExtender

FortiExtender edge device support requires a separate FortiSASE ThinEdge license per FortiExtender device. Contact your Fortinet Sales/Partner representative to purchase a FortiSASE ThinEdge license for each FortiExtender.

FortiSASE supports management and integration of a FortiExtender configured as a LAN extension. A FortiExtender with the LAN extension configuration allows a microbranch deployment. A microbranch deployment is a branch office with a LAN behind a FortiExtender with secure internet access over a backhaul connection to FortiSASE. By relying on FortiExtender instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser multidevice LAN environment.



When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Prerequisites

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for FortiExtender site-based remote users.

FortiCloud account prerequisites

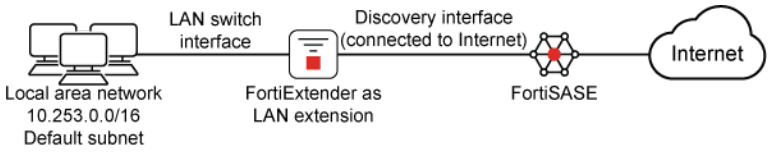
You must register FortiExtender devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

To activate FortiExtender management support on FortiSASE, you must purchase and apply a FortiSASE ThinEdge License to each FortiExtender device registered.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiExtender as a FortiSASE LAN extension configuration uses:



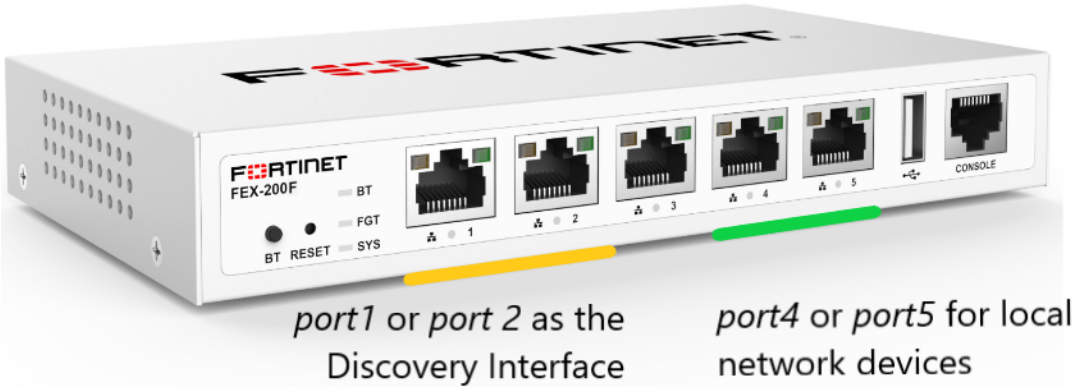
By default, using DHCP, FortiSASE dynamically assigns IP addresses to devices connected to the local network of the FortiExtender, that is, the LAN switch interface.

You should connect the FortiExtender's discovery interface to the internet. FortiExtender uses this interface for communication with FortiSASE. You can configure this interface to use DHCP or static IP addressing from the GUI or CLI.

For the FortiExtender 200F, specifically, note the following:

- Connecting the local network devices to port4 or port5 within the LAN switch interface is recommended.
- port1 or port2 are designated with the WAN role and you can use one or both ports as the discovery interface.

See the following picture for reference:



Connecting and logging into the FortiExtender 200F

To connect to the FortiExtender 200F using a computer and log into the FortiExtender GUI:

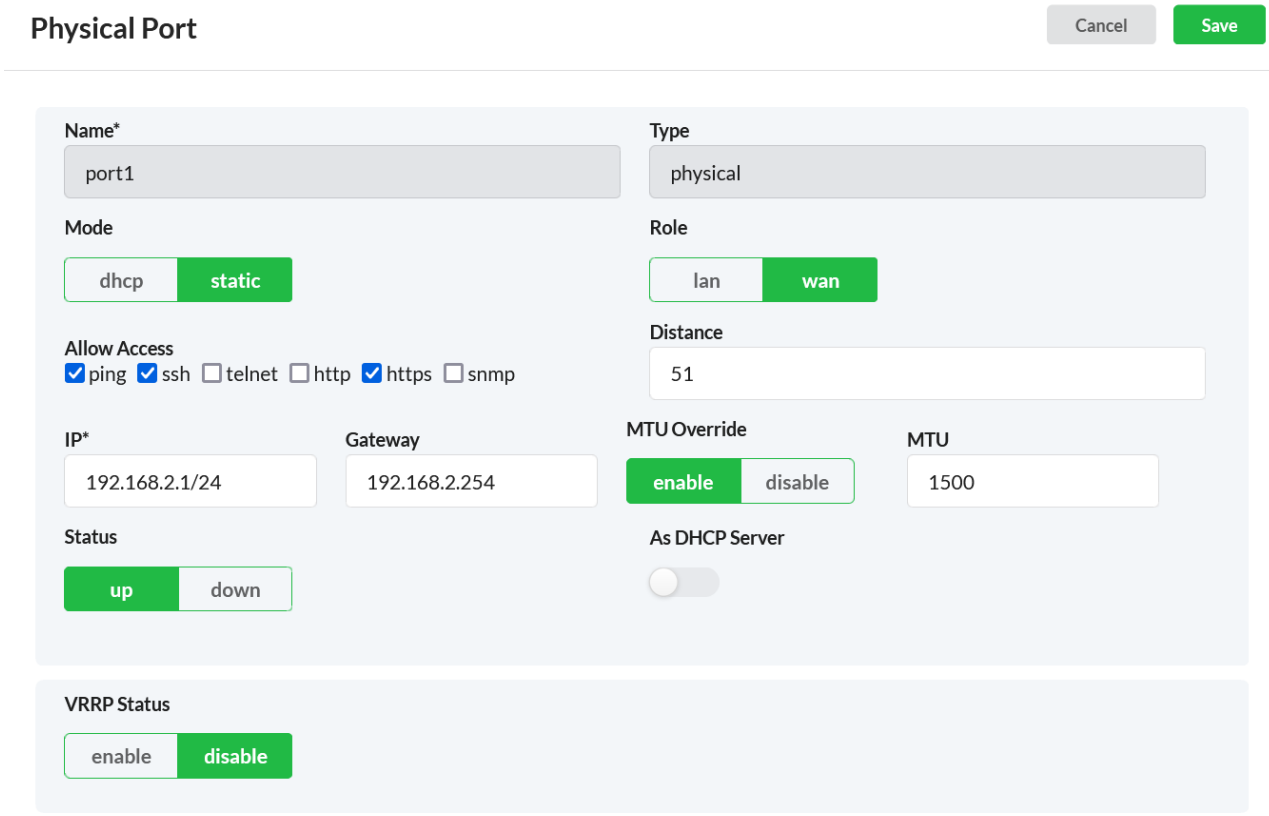
1. Use an Ethernet cable to connect a LAN port in the back of the FortiExtender to your computer's Ethernet port.
2. Configure the computer to be on the same subnet as the FortiExtender 200F by changing its IP address to 192.168.200.100 and the netmask to 255.255.255.0.
3. In a web browser, go to the default FortiExtender 200F web GUI address: http://192.168.200.99.
4. In the username and password fields, enter admin, then press *Enter*.

Configuring the discovery interface's IP address

You can configure the discovery interface's IP address via the FortiExtender GUI or CLI.

To configure the discovery interface's IP address via the GUI:

1. Log into the FortiExtender GUI as Connecting and logging into the FortiExtender 200F on page 34 describes.
2. Go to *Networking* > *Interface*.
3. Under *Physical Port*, select the port to configure as the discovery interface.
4. Click the pencil icon beside the desired port.
5. Under *Mode*, select *dhcp* or *static*. If you select *static*, configure the required IP address in the *IP* field, using IP address/subnet format, and the desired gateway settings in the *Gateway* field.
6. Click *Save*.



To configure the discovery interface's IP address via the CLI:

Use the following CLI commands where `<port>` is `port1` or `port2` on the FortiExtender 200F and `<mode>` is `dhcp` or `static`:

```
config system interface
  edit <port>
    set mode { dhcp | static }
    set ip <interface IP address/subnet>
    set gateway <gateway IP address for static IP address configuration>
```

```
  next
end
```

For example, to configure the FortiExtender 200F port1 with a static IP address and subnet of 192.168.2.1/24 and default gateway of 192.168.2.254, use the following CLI commands:

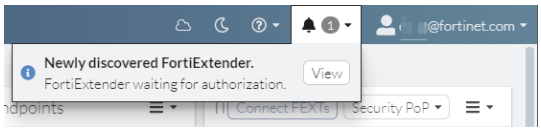
```
config system interface
  edit port1
    set mode static
    set ip 192.168.2.1/24
    set gateway 192.168.2.254
  next
end
```

SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

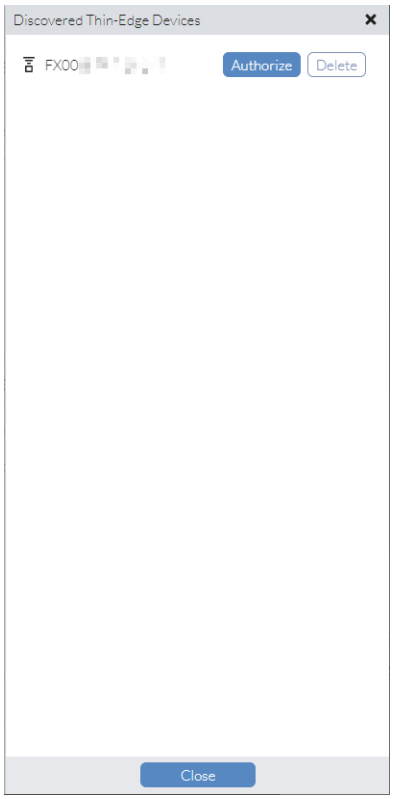
Viewing notifications for a new FortiExtender

When a new FortiExtender powers on, the bell icon in the header displays a notification about the new device. In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



A popup notification also displays.

Clicking *View* from the notifications displays a pane with the option to authorize or delete the FortiExtender.



Configuring FortiExtender as FortiSASE LAN Extension

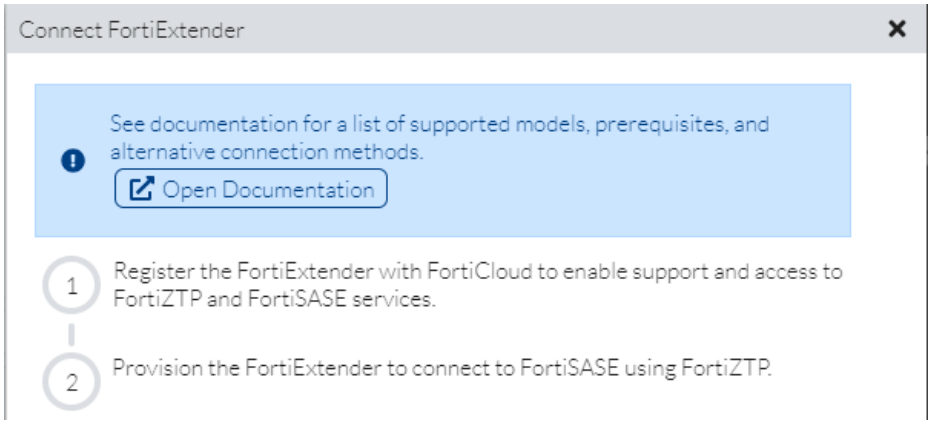
In *Edge Devices* > *FortiExtenders*, you can authorize, deauthorize, and delete FortiExtenders:

Connecting FortiExtender to FortiSASE using FortiZTP

Prior to connecting a FortiExtender to FortiSASE, you can view the instructions in the *Connect FEXTs* dialog in FortiSASE.

To view instructions to connect a FortiExtender to FortiSASE:

1. Go to *Edge Devices* > *FortiExtenders*.
2. Click *Connect FEXTs*. The instructions display.



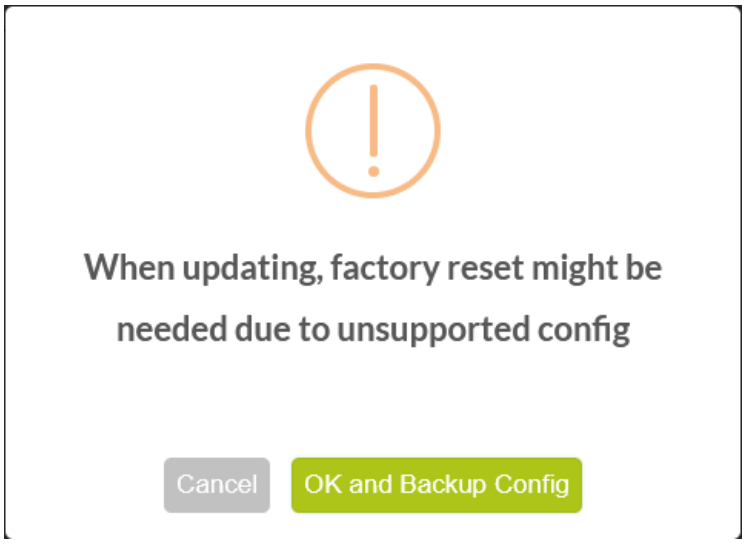
In addition to the instructions in the *Connect FEXTs* dialog, you generally must perform these preliminary steps to ensure proper connectivity:

1. Upgrade the FortiExtender to the latest firmware version known to work with FortiSASE. See SIA for site-based remote users.
2. Factory reset the FortiExtender device to ensure no prior configuration remains on the device.

To upgrade the FortiExtender to the latest firmware:

1. Connect and log into the FortiExtender GUI.
2. From the navigation bar, click *Settings*.
3. On top of the page, click *Firmware*.
4. In *Extender Upgrade*, select the desired OS firmware to upgrade to. Select one of the following:
   - *Local*: download the FortiExtender firmware image from the Fortinet Support Site and browse to its location locally on your machine.
   - *FortiCloud*: download and install images directly from FortiCloud.
5. After selecting the OS firmware to upgrade to, click the green up arrow to start the upgrade.

6. You see a warning message that upgrading may require a factory reset. Click *OK and Backup Config*.



7. FortiExtender prompts you to reboot to complete the firmware upgrade. Click *Restart Now* to complete the upgrade.

To factory reset the FortiExtender from the GUI:

1. Connect and log into the FortiExtender GUI.
2. Click the person icon in the top-right and select *Factory Reset*. FortiExtender prompts you to confirm the factory reset.
3. Click *OK* to confirm and perform the factory reset. A reboot occurs as part of the factory reset process.

To factory reset the FortiExtender from the CLI:

1. Access the console from the FortiExtender GUI navigation bar or by connecting a console cable to the FortiExtender and using terminal software.
2. Enter the following FortiExtender CLI command to factory reset the device: `execute factory-reset`
3. Confirm the factory reset when prompted by entering `y`:

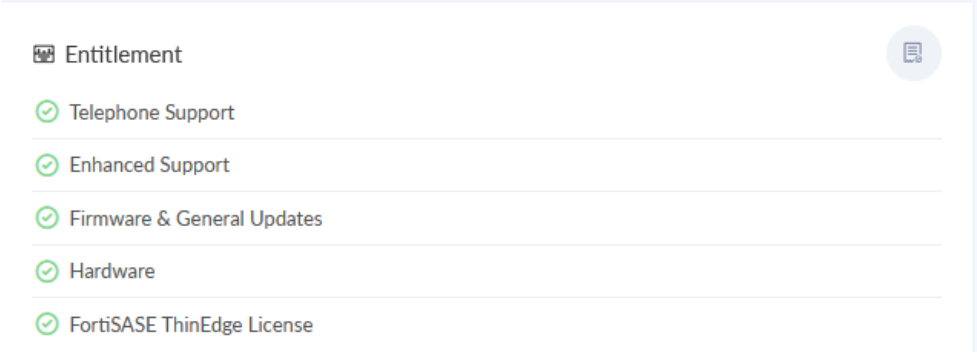
```
FX200F # execute factory-reset
The operation will do factory reset and then reboot the system!
Do you want to continue? (y/n)y
```

A reboot occurs as part of the factory reset process.

To register FortiExtender and FortiSASE license on FortiCloud:

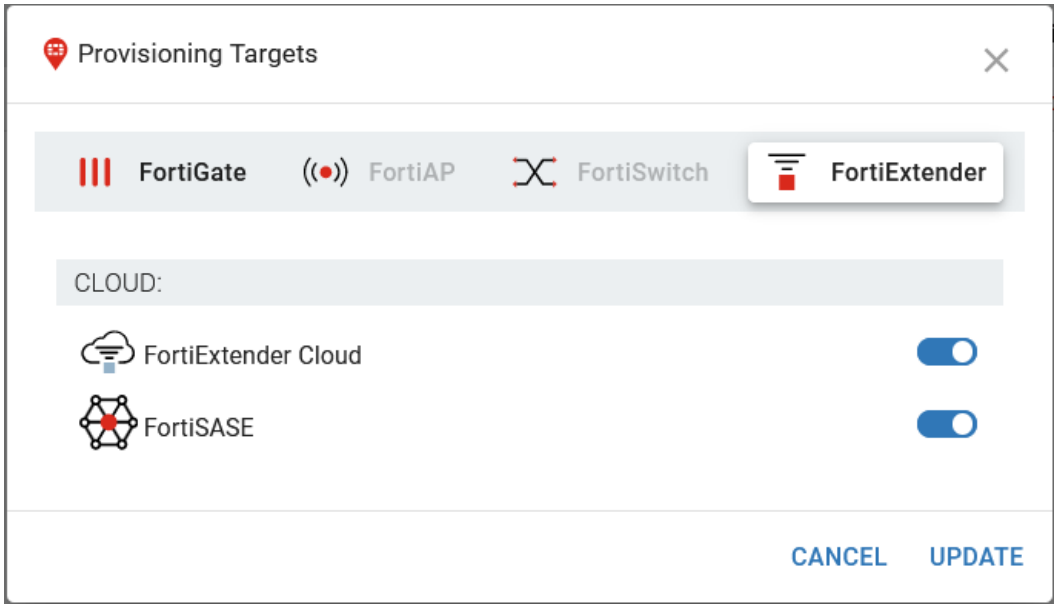
1. Sign in to your FortiCloud account.
2. Go to *Products* and click the *Register More* button.
3. In the *Register Product* dialog, in the *Registration Code* field, enter the FortiExtender serial number and follow the dialogs to complete registering the FortiExtender. For details on registering products, see Registering assets.
4. In the *Register Product* dialog, in the *Registration Code* field enter, the FortiSASE ThinEdge License registration code and follow the dialogs to complete registering the FortiSASE Thin Edge license. For details on registering products, see Registering assets.
5. Go to *Products* and *Product List* to confirm that the FortiExtender device and has been registered. Click the

FortiExtender serial number. Ensure that *Entitlement* lists FortiSASE ThinEdge License.



To provision a FortiExtender to FortiSASE using FortiZTP:

1. In FortiSASE, click *Services*. Under *Cloud Services*, click *FortiZTP*. The remaining steps are performed in FortiZTP.
2. Click the *Provisioning Settings* button on the right.
3. On the *FortiExtender* tab, ensure that *FortiSASE* is enabled.



4. Click *UPDATE*.
5. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiExtender, click the *Provision* icon.
   b. To provision multiple FortiExtenders, select the checkboxes for the desired FortiExtenders, then click the *PROVISION* button.
6. Under *TARGET LOCATION* in the *Provision devices* dialog, select FortiSASE. Only options that you have configured in *Provisioning Settings* appear in this dialog.
7. Do one of the following:
   a. Click *NEXT*. You can choose to associate the FortiExtender with a profile. Select the desired profile, then click *PROVISION NOW*.
   b. Click *PROVISION NOW*.

After completing the aforementioned steps, you can proceed to authorize the FortiExtender in FortiSASE as Authorizing a FortiExtender on page 44 describes.

Connecting a FortiExtender to FortiSASE using alternative connection methods

You can connect a FortiExtender to FortiSASE using alternative connection methods, namely via the FortiExtender GUI or CLI.

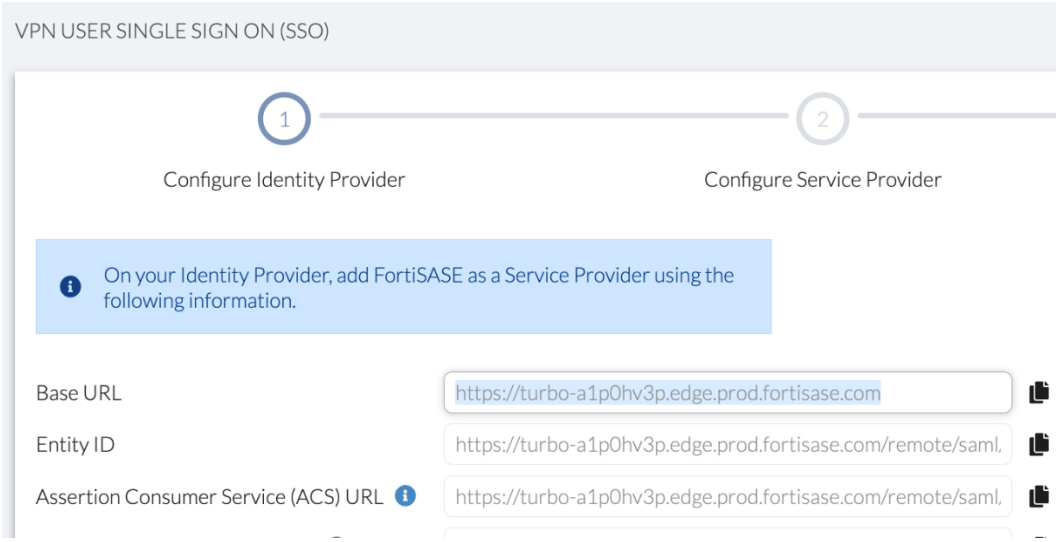
For ease of configuration, following the steps in Connecting FortiExtender to FortiSASE using FortiZTP on page 37 is recommended.

As a reference, this section describes alternative connection methods other than using FortiZTP.

Before using the FortiExtender GUI or CLI steps, you must obtain the FortiSASE domain name from FortiSASE.

To obtain the FortiSASE domain name from FortiSASE:

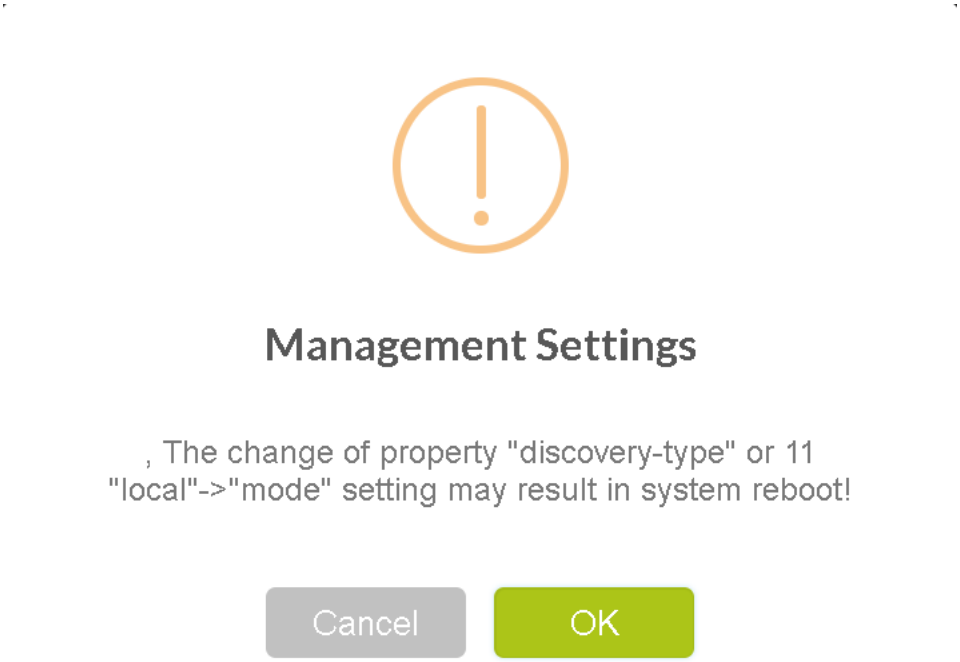
1. Go to *Configuration* > *VPN User SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo-a1p0hv3p.edge.prod.fortisase.com.



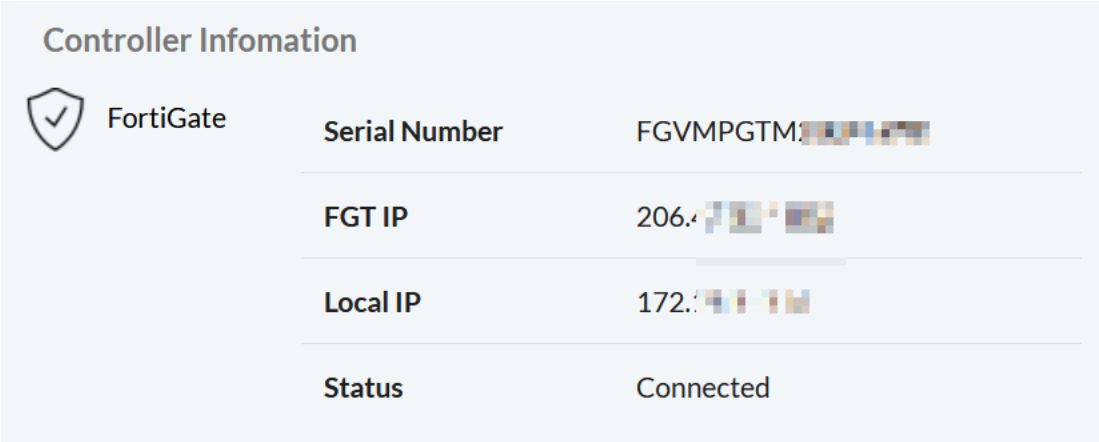
To connect a FortiExtender to FortiSASE via the GUI:

1. Log in to the FortiExtender GUI.
2. Go to *Settings* > *Management*.
3. Beside *Management Setup*, click the pencil icon to edit these settings and configure the following settings:
   a. *Controller*: *fortigate*
   b. *Discovery Type*: *static*
   c. *Discovery Interface*: <interface connected to the internet>
   d. For *Static Access Control Address*, click the pencil icon next to *ID 1* to edit this entry. Enter Server: <FortiSASE domain name here from *Connect FEXTs* dialog>. Click *Save*.
4. Click *Save*.

5. Click *OK* in the dialog to have changes take effect and reboot the FortiExtender.



6. To confirm the FortiExtender's connection to FortiSASE, log in to the FortiExtender GUI and go to *Dashboard*. Under *Controller Information*, confirm that *FGT IP* is non-zero, and *Status* is *Connected*.



To connect a FortiExtender to FortiSASE via the CLI:

The following commands are adapted from FortiExtender LAN extension in public cloud FGT-VM.

1. Connect FortiExtender to FortiSASE:

```
config system management
  set discovery-type fortigate
  config fortigate
    set ac-discovery-type static
    config static-ac-addr
      edit 1
        set server <FortiSASE domain name here from Connect FEXTs dialog>
```

```
      next
    end
    set discovery-intf port1
  end
end
```

2. To confirm the FortiExtender's connection to FortiSASE, run the `get extender status` command in the FortiExtender CLI. Confirm that `controller-addr` is non-zero and `management-state` is `CWWS_RUN`. The following shows sample output:

```
FX200FXXXXXXXXXX # get extender status
Extender Status
    name                 : FX200FXXXXXXXXXX
    mode                 : CAPWAP
    fext-addr            : 172.XX.XXX.XXX
    ingress-intf         : port1
    controller-addr      : 206.XX.XXX.XXX:5246
    controller-name      : FGXXXXXXXXXXXXXX
    uptime               : 0 days, 1 hours, 18 minutes, 31 seconds
    management-state     : CWWS_RUN
    base-mac             : AA:BB:CC:11:22:33
    network-mode         : lan-extension
    fgt-backup-mode      : backup
    discovery-type       : static
    discovery-interval   : 5
    echo-interval        : 30
    report-interval      : 30
    statistics-interval  : 120
    mdm-fw-server        : fortiextender-firmware.forticloud.com
    os-fw-server         : fortiextender-firmware.forticloud.com
```

Troubleshooting a FortiExtender that FortiSASE does not see

If after configuring the FortiExtender, FortiSASE does not see it, take the following troubleshooting steps.

To troubleshoot a FortiExtender that FortiSASE does not see:

1. Ensure that FortiExtender is updated to the latest firmware. See To upgrade the FortiExtender to the latest firmware: on page 38.
2. After updating the FortiExtender firmware, ensure you restore the device to its factory default settings, also known as perform a factory reset, by pressing and holding the Reset/Default button for more than five seconds.
   - For details on performing a factory reset using the FortiExtender GUI, see To factory reset the FortiExtender from the GUI: on page 39.
   - For details on performing a factory reset using the FortiExtender CLI, see To factory reset the FortiExtender from the CLI: on page 39.
   - For details on the Reset/Default button location on the FortiExtender 200F, see the FortiExtender 200F QuickStart Guide.
3. Ensure that the FortiExtender is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 33.
4. Connect your internet connection to port 1 and local LAN to ports 4-5. See Network topology on page 34.

After properly configuring and connecting a FortiExtender, it takes a few minutes to connect FortiExtender to FortiSASE, after which FortiSASE takes over DHCP and serves as your default gateway. Until then, traffic traverses your local internet connection.

Authorizing a FortiExtender

If FortiSASE does not find a *FortiSASE ThinEdge License*, it disables the *Authorization* > *Authorize* button and hovering over the *Authorize* button displays the *No authorization entitlements for FortiExtenders* tooltip. Therefore, only licensed FortiExtenders can be authorized.

Please ensure you apply a *FortiSASE ThinEdge License* to each FortiExtender to be managed by FortiSASE.

If the number of FortiExtender devices to be authorized exceeds the number of *FortiSASE ThinEdge Licenses* available, then the *Authorization* > *Authorize* button will be disabled and hovering over the *Authorize* button will display the tooltip “All X licensed FortiExtenders have been authorized. Deauthorize a device or purchase additional entitlements to authorize additional FortiExtenders” where X is the total number of registered entitlements for thin-edge management.

Proceed as advised by the tooltip to ensure your FortiExtenders can be managed by FortiSASE.

To authorize a FortiExtender:

1. Go to *Edge Devices* > *FortiExtenders*.
2. Select the desired FortiExtender.
3. Do one of the following:
   a. Under *Authorization*, click the *Authorize* button.
   b. Right-click the device and select *Authorization* > *Authorize*.
4. After authorization, FortiSASE displays the FortiExtender status as offline. Refresh the *FortiExtenders* page. The FortiExtender device status changes to online.

Deauthorizing a FortiExtender

To deauthorize a FortiExtender:

1. Go to *Edge Devices* > *FortiExtenders*.
2. Select the desired FortiExtender.
3. Do one of the following:
   a. Under *Authorization*, click the *Deauthorize* button.
   b. Right-click the device and select *Authorization* > *Deauthorize*.

After deauthorization, FortiSASE displays the FortiExtender status as *FortiCare Registered*.

Disconnecting a FortiExtender

If a FortiExtender device has been deregistered from the FortiCloud account, then disconnecting this device will remove the listed device from the FortiSASE *Edge Devices* > *FortiExtenders* page.

To disconnect a FortiExtender:

1. Go to *Edge Devices* > *FortiExtenders*.
2. Select the desired FortiExtender.
3. Do one of the following:
   a. Click the *Disconnect* button.
   b. Right-click the device and select *Disconnect*.

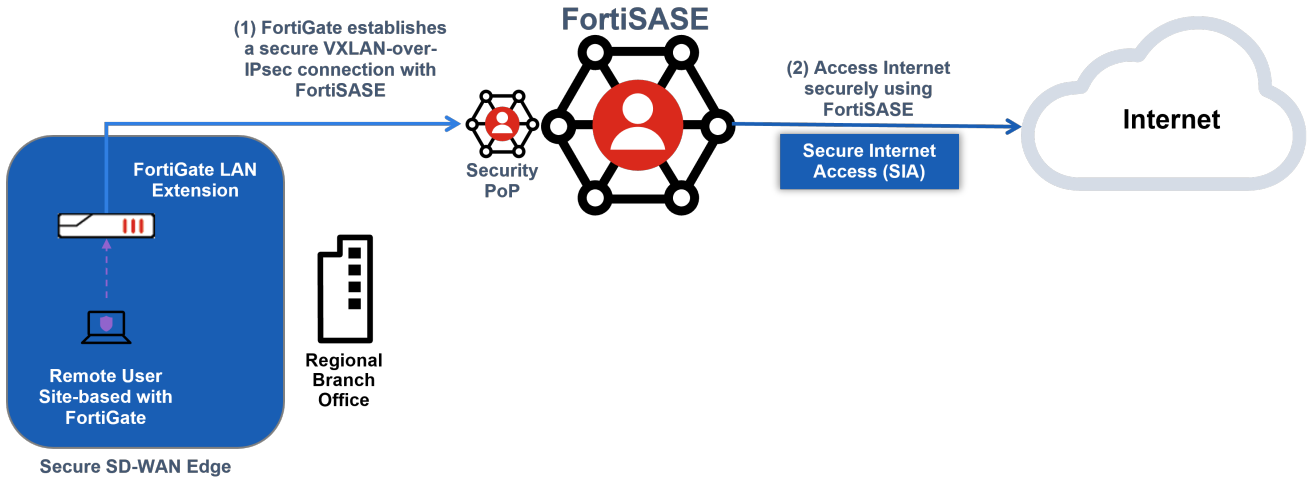
FortiGate

FortiGate SD-WAN as a secure edge requires a separate FortiSASE subscription license per FortiGate. All FortiGate F- and G-series desktop platforms below the 100 series running FortiOS 7.4.2 and later can support FortiSASE Secure Edge connectivity.

Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiGate.

You can configure a FortiGate SD-WAN device as a FortiSASE LAN extension, also known as a FortiGate Secure Edge, by setting up a VXLAN-over-IPsec tunnel between the FortiGate and FortiSASE. This creates a layer 2 network between FortiSASE and the network behind the remote FortiGate. In this use case, because the FortiGate is responsible for centralizing its remote users' site connectivity to the FortiSASE firewall-as-a-service (FWaaS), you only need to configure the endpoints in their IP settings to forward traffic to the FortiGate as the default gateway.

Therefore, this use case minimizes individual workstation or device setup because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based endpoints.



When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Prerequisites

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for FortiGate site-based remote users.

FortiCloud account prerequisites

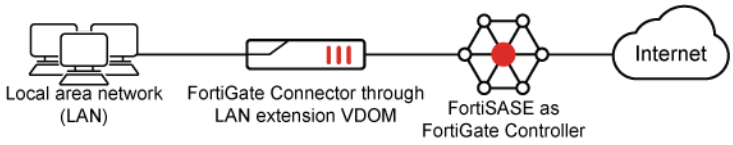
You must register FortiGate devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

To activate FortiGate management support on FortiSASE, you must purchase and apply a FortiSASE subscription license per FortiGate device registered. See the FortiSASE Ordering Guide.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiGate as a FortiSASE LAN extension configuration uses:



The FortiGate LAN extension feature is used in this topology where the FortiGate Connector is the on-premise FortiGate Secure Edge device and the FortiGate Controller is FortiSASE.

A new VDOM can be created on the FortiGate Connector and its type can be set to LAN extension. This configuration allows the VDOM to function as a FortiGate in LAN extension mode.

Connecting and logging into the FortiGate

For details on connecting and logging into the FortiGate GUI, see Connecting using a web browser.

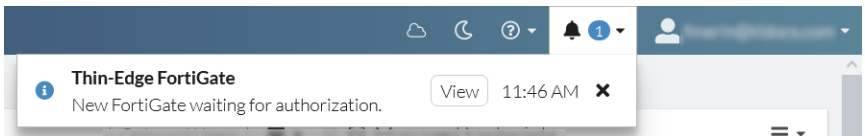
For details on connecting and logging into the FortiGate CLI, see Connecting to the CLI.

SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Viewing notifications for a new FortiGate

When a new FortiGate powers on, the bell icon in the header displays a notification about the new device. In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



Clicking *View* from the notifications, displays the FortiGate in the *Edge Devices* > *FortiGates* page.

Alternatively, you can see the number of FortiGates waiting for authorization beside *Edge Devices* > *FortiGates* in the navigation bar on the left.

Configuring FortiGate as FortiSASE LAN Extension

Connecting FortiGate to FortiSASE using the GUI and CLI

To connect the FortiGate as FortiSASE LAN extension or FortiGate secure edge, follow this configuration workflow:

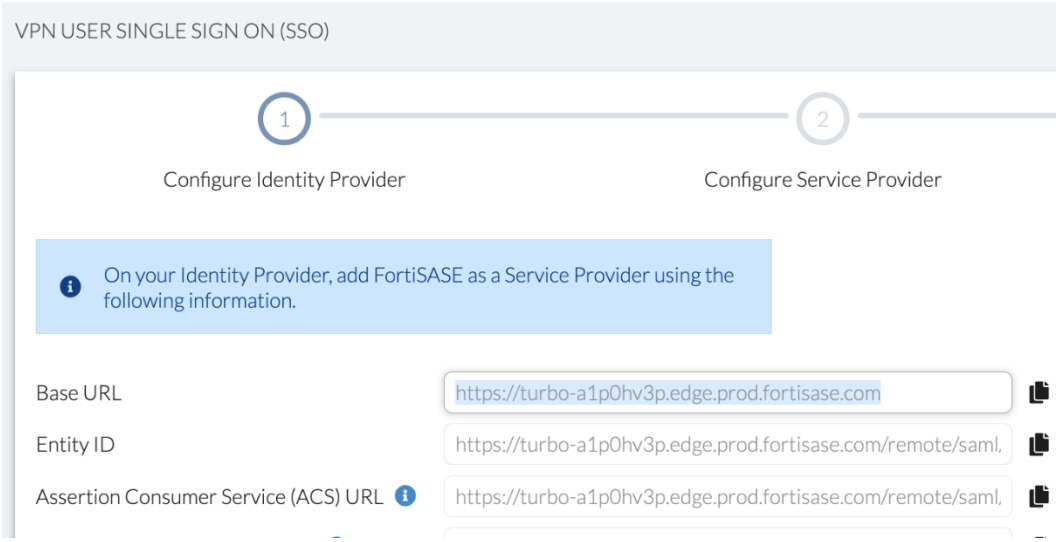
1. Obtain the FortiSASE domain name from FortiSASE.
2. Configure the FortiGate to connect to FortiSASE using the FortiSASE domain name.

For details on configuring the FortiGate secure edge to connect to FortiSASE using the GUI or CLI, see FortiGate secure edge to FortiSASE. In these configuration steps, the FortiGate secure edge fulfills the FortiGate connector role while FortiSASE fulfills the FortiGate controller role.

To obtain the FortiSASE domain name from FortiSASE:

1. Go to *Configuration* > *VPN User SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example,

the FortiSASE domain name is `turbo-a1p0hv3p.edge.prod.fortisase.com`.



Troubleshooting a FortiGate that FortiSASE does not see

If after configuring the FortiGate, FortiSASE does not see it, take the following troubleshooting steps:

To troubleshoot a FortiGate that FortiSASE does not see:

1. Ensure that the FortiGate is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 46.
2. Ensure that the FortiGate is registered with a FortiSASE subscription license in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 46.
3. Verify the IPsec tunnels' phase 1 and phase 2 negotiations on the FortiGate Connector:

```
# diagnose vpn ike gateway list
# diagnose vpn tunnel list
```

4. Verify the LAN extension status on the Connector:

```
Connector-FGT (lan-ext) # get extender lanextension-vdom-status
Control-Channel:
        controller ip: 1.1.1.1
        controller port: 5246
        controller name: FGVMPGTM00000ABC
        missed echo: 0
        up time(seconds): 75194
        status: EXTWS_RUN
Data-Channel:
uplink [0]: wan1
        IPsec tunnel ul-wan1
        VxLAN interface vx-wan1
downlink [0]: internal1
downlink [1]: lan-ext-link1
```

In this example, the Connector is in a working state.

Authorizing a FortiGate

If no FortiSASE subscription license is found for a FortiGate, then the *Authorization* > *Authorize* button will be disabled and hovering over the *Authorize* button will display the tooltip “No authorization entitlements for this Device”. Therefore, only licensed FortiGates can be authorized.

Ensure you apply a FortiSASE subscription license to each FortiGate to be managed by FortiSASE.

To authorize a FortiGate:

1. Go to *Edge Devices* > *FortiGates*.
2. Select the desired FortiGate.
3. Do one of the following:
   a. Under *Authorization*, click the *Authorize* button.
   b. Right-click the device and select *Authorization* > *Authorize*.
4. After authorization, FortiSASE displays the FortiGate status as *Offline*. Refresh the *FortiGates* page. The FortiGate device status changes to *Online*.

Deauthorizing a FortiGate

To deauthorize a FortiGate:

1. Go to *Edge Devices* > *FortiGates*.
2. Select the desired FortiGate.
3. Do one of the following:
   a. Under *Authorization*, click the *Deauthorize* button.
   b. Right-click the device and select *Authorization* > *Deauthorize*.

   After deauthorization, FortiSASE displays the FortiGate status as *FortiCare Registered*.

Disconnecting a FortiGate

If a FortiGate device has been deregistered from the FortiCloud account, then disconnecting this device will remove the listed device from the FortiSASE *Edge Devices* > *FortiGates* page.

To disconnect a FortiGate:

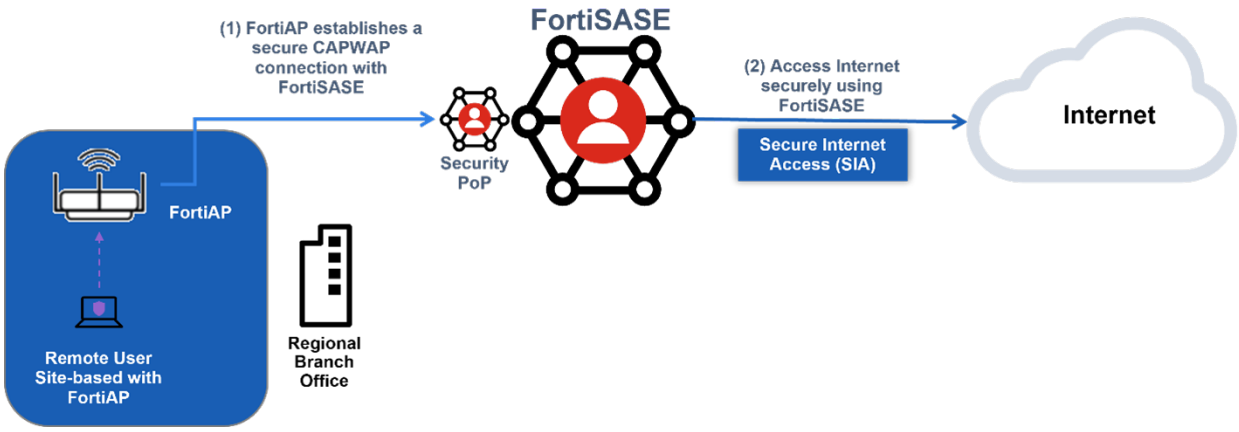
1. Go to *Edge Devices* > *FortiGate*.
2. Select the desired FortiGate.
3. Do one of the following:
   a. Click the *Disconnect* button.
   b. Right-click the device and select *Disconnect*.

FortiAP

FortiAP edge device support requires a separate FortiSASE subscription license per FortiAP. This feature supports FortiAP 231F and 431F devices running FortiAP firmware 7.2.4 and later.

Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiAP.

FortiSASE supports management and integration of a FortiAP as an edge device allowing for a micro-branch deployment. A micro-branch deployment is a branch office with a FortiAP managed over a backhaul connection to FortiSASE that provides secure internet access to Wi-Fi clients. By relying on FortiAP instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user single-device FortiClient endpoint case to a multiuser multidevice Wi-Fi environment.



When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Prerequisites

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for FortiAP site-based remote users.

FortiCloud account prerequisites

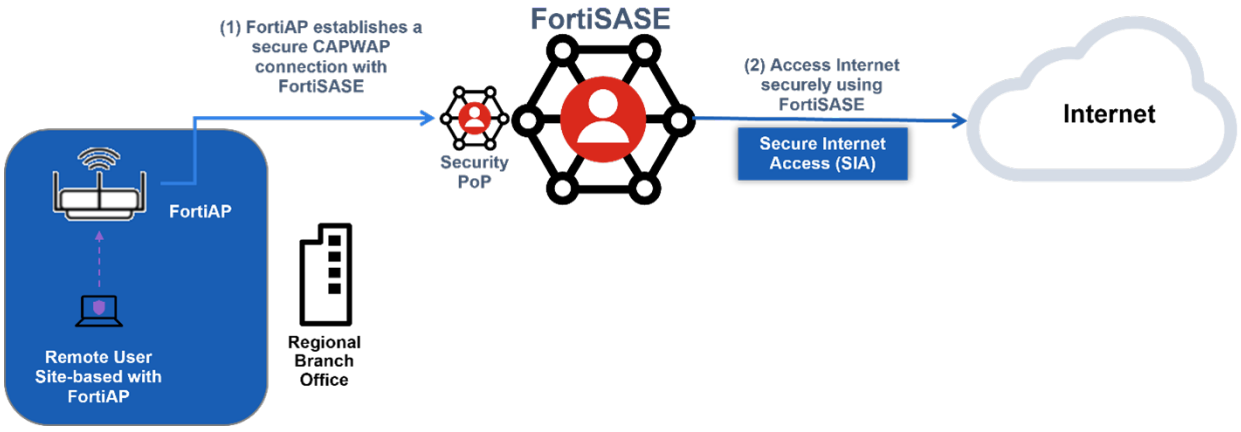
You must register FortiAP devices to the same FortiCloud account used to log into FortiSASE before using this feature.

To activate FortiAP management support on FortiSASE, you must purchase and apply a FortiSASE subscription license to each FortiAP device registered.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts the network topology that the FortiAP as a FortiSASE edge device configuration uses:



A CAPWAP tunnel is established between FortiSASE and the FortiAP device.

There are two channels inside the CAPWAP tunnel:

- Control channel for managing traffic, which is always encrypted by DTLS.
- Data channel for carrying client data packets, which can be configured to be encrypted or not.

For a FortiAP to be managed by FortiSASE, the data channel is encrypted using an IPsec VPN tunnel between FortiSASE and the FortiAP that carries CAPWAP data packets and includes the FortiAP serial number within this tunnel.

By default, using DHCP, FortiSASE dynamically assigns IP addresses to Wi-Fi devices connected to the FortiAP.

Connecting and logging into the FortiAP

You can use one of these methods for connecting and logging into the FortiAP device:

- Connect to the FortiAP using a computer with a direct wired connection to the FortiAP
- Reset the FortiAP to allow access using FortiAP Configuration mode

To connect to the FortiAP using a computer with a direct wired connection for GUI or CLI access:

1. Connect an Ethernet cable from the LAN port in the back of the FortiAP to one of the following:
   a. FortiSwitch with Power-over-Ethernet (PoE) enabled on the port and then use another Ethernet cable to connect a computer's Ethernet port to one of the free ports on the FortiSwitch.
   b. PoE injector and then use another Ethernet cable to connect from the PoE injector to a computer's Ethernet port.
2. Configure the computer to be on the same subnet as the FortiAP by changing its IP address to 192.168.1.1 and the netmask to 255.255.255.0.
3. Access the GUI or CLI using 192.168.1.2:
   a. In a web browser, go to the default FortiAP web GUI address: https://192.168.1.2 .
   b. Using SSH, go to 192.168.1.2.
4. In the *Username* field, enter admin and keep the password blank if this is a new setup. Otherwise, in the *Password* field, enter the password associated with the admin account.
5. Create a new password that adheres to the listed password policy and then click *Change Password*.

To reset the FortiAP to use FortiAP Configuration mode for GUI or CLI access:

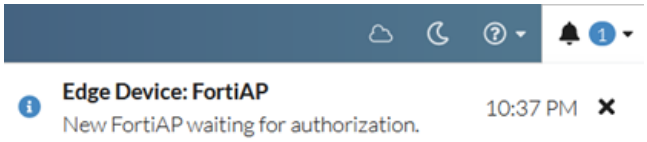
1. Ensure that the FortiAP is booted up.
2. Use a pin to push and hold the reset button for five to ten seconds. FortiAP reboots and then enters Configuration mode. FortiAP starts to broadcast an open security SSID `FAP-config-<serial-number>`, for example `FAP-config-FP421F0000000000`.
3. Access the GUI or CLI of the FortiAP Configuration mode using 192.168.100.1:
   a. In a web browser, go to the default FortiAP web GUI address: https://192.168.100.1 .
   b. Using SSH, go to 192.168.100.1
4. In the *Username* field, type admin.
5. In the *Password* field, type the password associated with the admin account.

SSL deep inspection for site-based users

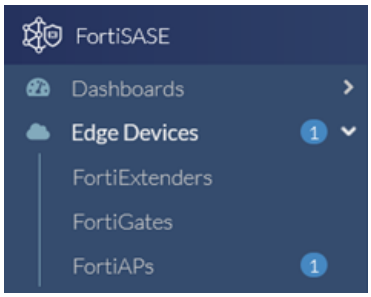
When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Viewing notifications for a new FortiAP

When a new FortiAP powers on, the bell icon in the header displays a notification about the new device.



In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



Configuring FortiAP as FortiSASE edge device

In *Edge Devices* > *FortiAPs*, you can configure FortiAPs:

- Connecting a FortiAP to FortiSASE using FortiZTP on page 53
- Managing FortiAPs on page 54
- Editing a FortiAP profile on page 57

- Creating a FortiAP profile and applying it to a FortiAP on page 59
- Creating an SSID on page 59
- Troubleshooting a FortiAP that FortiSASE does not see on page 62

Typically, the configuration workflow for a FortiAP as a FortiSASE edge device is as follows:

1. Connect the FortiAP to FortiSASE using FortiZTP.
2. Log into FortiSASE and view notifications confirming that FortiSASE sees the FortiAP.
3. Authorize the FortiAP. If needed, FortiSASE will automatically upgrade the FortiAP device firmware to the latest supported version.
4. Create an SSID for your wireless network.
5. Edit the default FortiAP profile to configure desired radio settings, including whether the radio will apply to all SSIDs or selected SSIDs.

Connecting a FortiAP to FortiSASE using FortiZTP

This section requires the FortiAP device to run a supported firmware version. See SIA for FortiAP site-based remote users.

If the FortiAP device runs an unsupported version, then it must be upgraded to a supported version first. See Upgrading to a supported FortiAP firmware version using alternative connection methods on page 64.

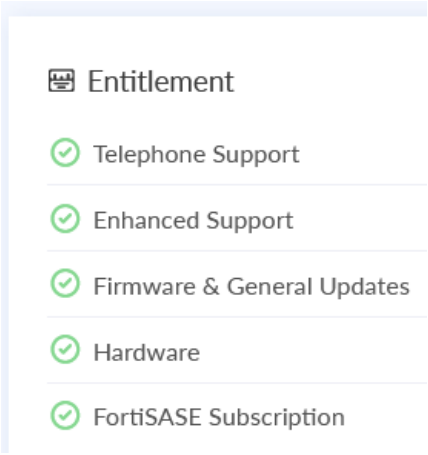
The following configuration workflow is required for connecting a FortiAP to FortiSASE:

1. Register FortiAP and FortiSASE license on FortiCloud.
2. Provision a FortiAP to FortiSASE using FortiZTP.

To register FortiAP and FortiSASE license on FortiCloud:

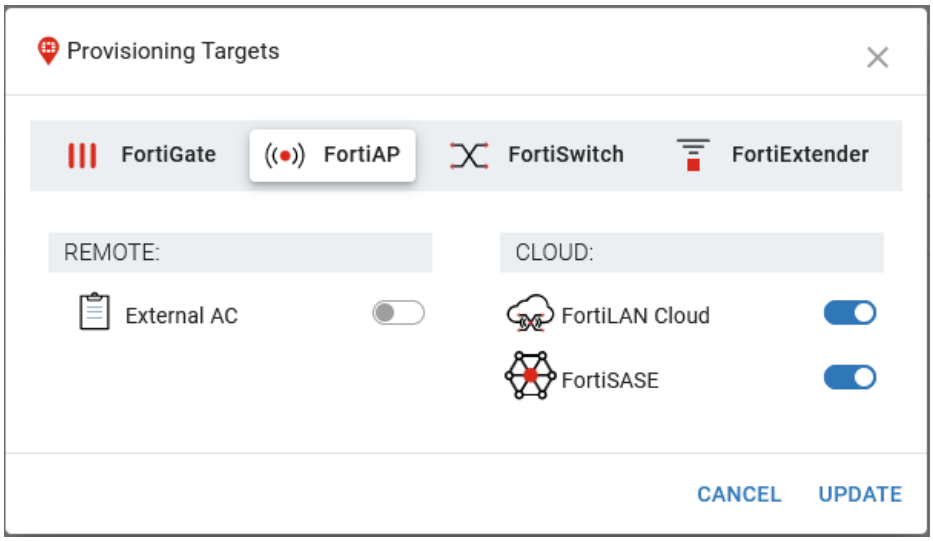
1. Sign in to your FortiCloud account.
2. Go to *Products* and click *Register More*.
3. In the *Register Product* dialog, in the *Registration Code* field, enter the FortiAP serial number and follow the dialogs to complete registering it. You require physical access to the FortiAP device because registration requires the cloud key on the back label. See Registering assets.
4. Repeat step 3 with the FortiSASE Subscription License registration code.
5. Go to *Products* and *Product List* to confirm that you registered the FortiAP device. Click the FortiAP serial number.

Ensure that *Entitlement* lists *FortiSASE Subscription*.



To provision a FortiAP to FortiSASE using FortiZTP:

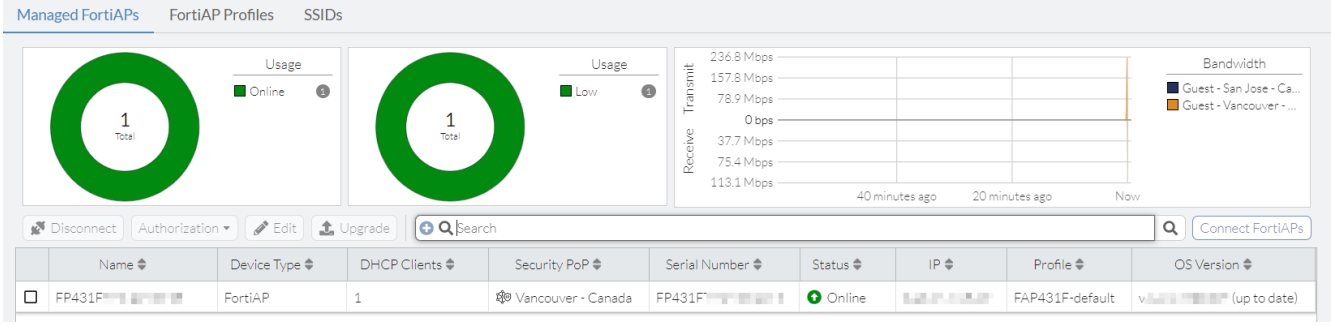
1. In FortiSASE, click *Services*. Under *Cloud Services*, click *FortiZTP*. You perform the remaining steps in FortiZTP.
2. In FortiZTP, click *Setting*.
3. On the *FortiAP* tab, ensure that *FortiSASE* is enabled.



4. Click *UPDATE*.
5. On the *UNPROVISIONED* tab, do the following:
   - To provision a single FortiAP, click *Provision*.
   - To provision multiple FortiAPs, select the checkboxes for the desired FortiAPs, then click *PROVISION*.
6. Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiSASE*. Only options that you have configured in *Provisioning Settings* appear in this dialog.
7. Click *PROVISION NOW*.
8. In the prompt that mentions the provision process started for devices, click *OK*.

Managing FortiAPs

You can manage a FortiAP device from *Edge Devices* > *FortiAPs* in the *Managed FortiAPs* tab.



The *Managed FortiAPs* tab presents these charts for monitoring:

- Usage chart with a summary of FortiAP device status
- Usage chart with a summary of FortiAP devices based on client load based on the number of clients connected (supported FortiAP devices have two Wi-Fi radios):
  - High: more than 110 clients
  - Average: 60-110 clients
  - Low: fewer than 60 clients
- Bandwidth chart displaying inbound FortiAP edge device traffic per SSID and security PoP

From this page, you can perform these tasks:

Authorizing a FortiAP and upgrading to a supported FortiAP firmware version

If FortiSASE does not find a FortiSASE subscription license, it disables the *Authorization* > *Authorize* button and hovering over the *Authorize* button displays *No authorization entitlements for this Device*. Therefore, you can only authorize licensed FortiAPs.

Ensure you apply a FortiSASE subscription license to each FortiAP for FortiSASE to manage.

If needed, the FortiAP automatically upgrades to the latest FortiAP firmware version. The FortiAP must reboot as part of the upgrade. Wireless endpoints already connected to the FortiAP may experience temporary connectivity loss.

To authorize a FortiAP:

1. Go to *Edge Devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top.
2. Select the desired FortiAP.
3. Do one of the following:
   - Under *Authorization*, click the *Authorize* button.
   - Right-click the device and select *Authorization* > *Authorize*.
4. After authorization, FortiSASE displays the FortiAP status as *Offline*. Refresh the *FortiAPs* page. The FortiAP device status changes to *Online*. If needed, upon device authorization, FortiSASE automatically upgrades the FortiAP edge device to the latest supported FortiAP firmware release. The device must be authorized and online for the upgrade to take place.
   - The device must be running an older FortiAP firmware release than the latest supported version.
   - The device will need to reboot as part of the upgrade. Wireless endpoints already connected to the device may

experience a temporary loss of connectivity.
- It takes around 15-20 minutes before an upgrade is performed.

5. After 15-20 minutes, go to the *Managed FortiAPs* tab and observe the *OS Version* field reflects the latest FortiAP firmware version that the device was upgraded to.

Deauthorizing a FortiAP

To deauthorize a FortiAP:

1. Go to *Edge Devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top.
2. Select the desired FortiAP.
3. Do one of the following:
   - Under *Authorization*, click the *Deauthorize* button.
   - Right-click the device and select *Authorization* > *Deauthorize*.

After deauthorization, FortiSASE displays the FortiAP status as *FortiCare Registered*.

Disconnecting a FortiAP

If a FortiAP device has been deregistered from the FortiCloud account, then disconnecting this device will remove the listed device from the FortiSASE *Edge Devices* > *FortiAPs* page.

To disconnect a FortiAP:

1. Go to *Edge Devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top..
2. Select the desired FortiAP.
3. Do one of the following:
   a. Click the *Disconnect* button.
   b. Right-click the device and select *Disconnect*.

Editing a FortiAP

From *Edge Devices* > *FortiAPs* under the *Managed FortiAPs* tab, by selecting a FortiAP device and clicking *Edit*, you can edit these settings:

Field	Description
Name	Enter a name for the FortiAP.
Authorized	Authorization state of the FortiAP.
FortiAP Profile	FortiAP profile applied to this FortiAP.
Enable LEDs	Select if you want LEDs on the FortiAP to be enabled (default) or disabled.
Login Password	Select if you want set a new AP login password or leave the password unchanged.

Upgrading to the latest supported FortiAP firmware version after authorization

This procedure describes how to upgrade the FortiAP to the latest supported firmware version after the initial authorization.

The FortiAP device must be authorized and online for the upgrade to take place. The FortiAP will need to reboot as part of the upgrade. Wireless endpoints already connected to the FortiAP may experience a temporary loss of connectivity.

To upgrade to a supported FortiAP firmware version after authorization:

1. Go to *Edge Devices* > *FortiAPs* and click the *Managed FortiAPs* tab at the top.
2. Select the desired FortiAP.
3. Do one of the following:
   - Click the *Upgrade* button.
   - Right-click the device and select *Upgrade*.
4. FortiSASE displays a prompt warning of a FortiAP reboot and temporary loss of connectivity for wireless endpoints already connected to the FortiAP, and lists the FortiAP firmware version to be upgraded to. Click *OK* to continue with the FortiAP firmware upgrade.
5. Observe the message at the top-right of the screen: *Request to upgrade the FortiAP to latest firmware successful.*
   - The device must be running an older FortiAP firmware release than the latest supported version.
   - The device will need to reboot as part of the upgrade. Wireless endpoints already connected to the device may experience a temporary loss of connectivity.
   - It takes around 15-20 minutes before an upgrade is performed.
6. After 15-20 minutes, go to the *Managed FortiAPs* tab and observe the *OS Version* field reflects the latest FortiAP firmware version that the device was upgraded to.

Editing a FortiAP profile

When you authorize a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). The FortiAP profile defines the entire configuration for the AP.

From *Edge Devices* > *FortiAPs* under the *FortiAP Profiles* tab, you can create a new FortiAP profile or edit an existing default FortiAP profile.

Typically, you will edit an existing default FortiAP profile by selecting the profile and clicking *Edit*.

General FortiAP profile options

Field	Description
Name	Enter a name for the FortiAP profile
Model	Select the FortiAP model to which this profile applies. Currently 431F or 231F
Deployment Location	Select where the FortiAP is being installed either indoor or outdoor. You can override the default designation of the FortiAP to change the available channels based on your region.
Country/Region	Select the country or region to apply the Country Code for where the FortiAP will

Field	Description
	be used.
Login Password	Select if you want set a new AP login password or leave the password unchanged.
Client load balancing	Select a handoff type as needed. See Wireless client load balancing for high-density deployments.
802.1x authentication	Enable if you want to configure the FortiAP to act as a 802.1x supplicant to authenticate against the server using EAP-FAST, EAP-TLS or EAP-PEAP (see Configuring 802.1X supplicant on LAN).

Radio-specific profile options

Field	Description
Mode	Select the type of mode: • *Disabled*: radio is disabled. • *Access Point*: platform is an access point.
Band	Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11ax/n/g" means 802.11ax **and** 802.11n **and** 802.11g.
Channel Width	Select channel width for 802.11ax or 802.11n on 5 GHz. For optimal performance on supported radios, *Channel Width* is selected as 80 MHz by default for the default profile and for new profiles.
Short Guard Interval	Select to enable the short guard interval for 802.11ax or 802.11n on 5 GHz.
Channel Plan	For 2.4 GHz radios, select if you want to automatically configure a Channel plan or if want to select custom channels. • *Three Channels*: automatically selects channel 1, 6, and 11. • *Four Channels*: automatically selects channels 1, 4, 8, and 11. • *Custom*: select custom channels.
Channels	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in *Band*. By default, for 5 GHz radios all available channels are enabled.
Transmit Power Mode	Select how you want to determine transmit power: • *Percent*: transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. • *dB*m: transmit power is setting using a dBm value. • *Auto*: set a range of dBm values and the power is set automatically.
Transmit Power	Specify either the minimum and maximum Transmit power levels in dBm or as a percentage.
SSIDs	Select SSIDs to use for this radio either *All* or *Specify* with selected SSIDs added to a list.

Field	Description
	If SSIDs is configured to *All* for a radio, then click on *View Enabled SSIDs* to display a slide-in listing *Enabled SSIDs*. You may *Create*, *Edit*, or *Delete* SSIDs from this slide-in.
Monitor Channel Utilization	Select to enable monitoring channel utilization.

Creating a FortiAP profile and applying it to a FortiAP

You can also choose to create new FortiAP profiles by clicking *Create* for the purpose of overriding specific settings for individual FortiAPs. You cannot update the name, model, and country/region of a profile once you save it.

To assign a newly created FortiAP profile:

1. Go to *Edge Devices* > *FortiAPs*.
2. On the *Managed FortiAPs* tab, select a FortiAP device and click *Edit*.
3. For the *FortiAP profile* field, from the dropdown list, select the desired FortiAP profile to apply to this FortiAP.

Creating an SSID

You can configure your wireless network by defining one or more SSIDs to which your users can connect. FortiSASE uses IP address management (IPAM) to automatically configure IP/Netmask settings for an SSID.

For FortiSASE instances with the FortiAP 431F promo subscription only, a default SSID *Guest-SASE* is created with default password *FortiSASE*.

If secure private access (SPA) is configured, FortiSASE includes a policy that denies SPA access from wireless endpoints connected to this guest SSID.

General SSID settings

Field	Description
Name	Enter a name for the SSID interface.
Traffic Mode	*Tunnel* — (Tunnel to Wireless Controller) Data for WLAN passes through WiFi Controller. This is the default. Currently this is the only mode supported.
Status	SSID interface status.

WiFi Settings

Field	Description
SSID	Enter the SSID.
Client Limit	Limit the number of clients allowed in the SSID.
Broadcast SSID	Disable broadcast of SSID. By default, the SSID is not broadcast.[FM1]

WiFi Security

Field	Description
Mode	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. • *WPA2 Personal*: WPA2 is WiFi Protected Access version 2. Users use a pre-shared key (password) to obtain access. • *WPA2 Enterprise*: similar to WPA2 Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password. • *WPA3 Enterprise Only*: WPA3 enterprise with Protected Management Frames (PMF) mandatory. Best used for enterprise networks. Each user is separately authenticated by user name and password.
Pre-shared Key	Available only when *Mode* is *WPA2 Personal*. Preshared key must be 8 to 63 characters long.
Authentication	Available only when *Mode* is *WPA2 Enterprise* or *WPA3 Enterprise Only*. Select one of the following: • *RADIUS Server*: select the RADIUS server that will authenticate the clients. • *User Groups*: select the local user group(s) that can authenticate.

Example: Configuring an SSID using WPA2 Enterprise with a local user group

This example configures a Staff SSID with WPA2 Enterprise and a local user group for user authentication of staff users. This example requires a FortiAP edge device to already be connected to and authorized within FortiSASE. You can use this example to configure WPA3 Enterprise Only instead of WPA2 Enterprise.

The configuration workflow is as follows:

1. Create local users.
2. Create a local user group.
3. Create an SSID to use WPA2 Enterprise with the local user group.
4. Verify WPA2 Enterprise user authentication upon connecting to the SSID.

To create local users:

1. Go to *Configuration* > *Users & Groups*.
2. Select *User*.
3. Enter the *Email* of the new user. This will be the username of the new user.
4. Click *OK*. The new user will receive an email prompting them to activate the new account and to set a new password.
5. Repeat steps 1 to 4 to add more local users.

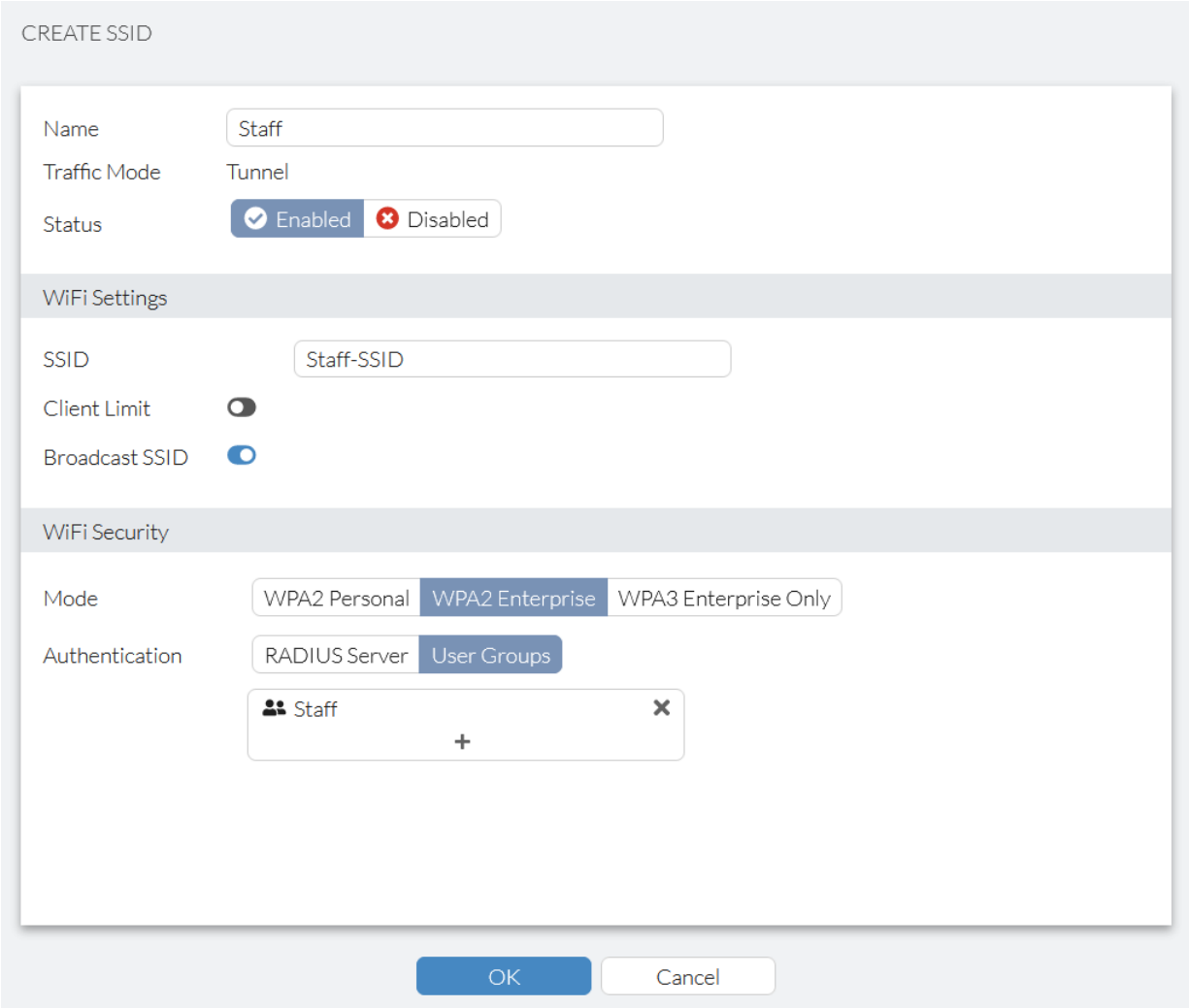
To create a local user group:

1. Go to *Configuration* > *Users & Groups*.
2. Select *User Group*.
3. Enter the *Name* of the new user group, for example, *Staff*.

4. For *Users*, click + and in the slide-in select the newly created local users to add to the local user group. Click *Close*.
5. Click *OK*.

To create an SSID to use WPA2 Enterprise with the local user group:

1. Go to *Edge Devices* > *FortiAPs*.
2. On the *SSIDs* tab, click *+Create*.
3. In the *Create SSID* page, do the following:
   a. Enter the *Name* of the SSID used for identifying the SSID in FortiSASE, for example, *Staff*.
   b. In *WiFi Settings*, configure the following:
      i. Enter the *SSID* name to be seen by wireless clients, for example, *Staff-SSID*.
      ii. Enable *Broadcast SSID*, if desired.
   c. In *WiFi Security*, configure the following:
      i. For *Mode*, select *WPA2 Enterprise*.
      ii. For *Authentication*, select *User Groups*.
      iii. Click +. In the slide-in, select the local user group created previously. In this example, it is *Staff*.
   d. Click *OK*.



To verify WPA2 Enterprise user authentication upon connecting to the SSID:

1. On a wireless client device, connect to the SSID, for example, *Staff-SSID*.
2. When prompted to continue connecting, click *Connect* to proceed.
3. Upon connection, you will be prompted to enter your user name and password. If you are using Windows, deselect *Use my Windows user account* and enter one of the local usernames and passwords to proceed.
4. Click *OK*.
5. Click *Connect*. Once connected, you should see *Connected, Secured* next to the SSID if you are using Windows. You should now be able to securely access the Internet through the SSID and FortiAP edge device managed by FortiSASE.

Troubleshooting a FortiAP that FortiSASE does not see

If after configuring the FortiAP, FortiSASE does not see it, take the following troubleshooting steps.

To troubleshoot a FortiAP that FortiSASE does not see:

1. Ensure that the FortiAP is registered in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 50.
2. Ensure that the FortiAP is registered with a FortiSASE subscription license in the same FortiCloud account as FortiSASE. See FortiCloud account prerequisites on page 50.
3. Ensure that after you connect the FortiAP to a wired network that it is getting a valid IP address, can access the internet, and can connect to the FortiSASE wireless controller. By default, the FortiAP obtains a LAN IP using DHCP. You can connect to the FortiAP CLI using a serial console connection and serial terminal software to perform these steps:
   a. Check the FortiAP LAN IP address and netmask, and default gateway, respectively, using these commands:

      ```
      ifconfig br0
      route
      ```

   b. Ping the FortiSASE domain name using `ping <FortiSASE domain name>` and then cancel it using Ctrl+C.
   c. Check the FortiAP has a valid CAPWAP connection to the wireless controller using this command:

      ```
      FortiAP-431F # cw_diag -c acs
      WTP Configuration
          name                  : FortiAP-431F
          loc                   : N/A
          ap mode               : thin AP
          ...
      ACS 0 info
          wcha info             : mode=0 max=10 wait=10 peer_cnt=0
          acPri                 : 1
          fsm-state             : RUN 768
          ac-ip-addr            : 154.52.4.72:5246,5247        DNS
          ac-name               : FGVMABCD00000EFG
          ...
          data-chan-sec-oper    : ipsec-sn
          ...

      ACS 1 info
          wcha info             : mode=0 max=0 wait=0 peer_cnt=0
          acPri                 : 2
          fsm-state             : START 796
      ```

```
ac-ip-addr            : 0.0.0.0:0,0         UNKNOWN
ac-name               :
...
```

4. For additional troubleshooting steps, refer to these topics as a reference only:
   a. Connecting a FortiAP to FortiSASE using alternative connection methods on page 63
   b. Upgrading to a supported FortiAP firmware version using alternative connection methods on page 64

Connecting a FortiAP to FortiSASE using alternative connection methods

You can connect a FortiAP to FortiSASE using alternative connection methods, namely, using the FortiAP GUI or CLI.

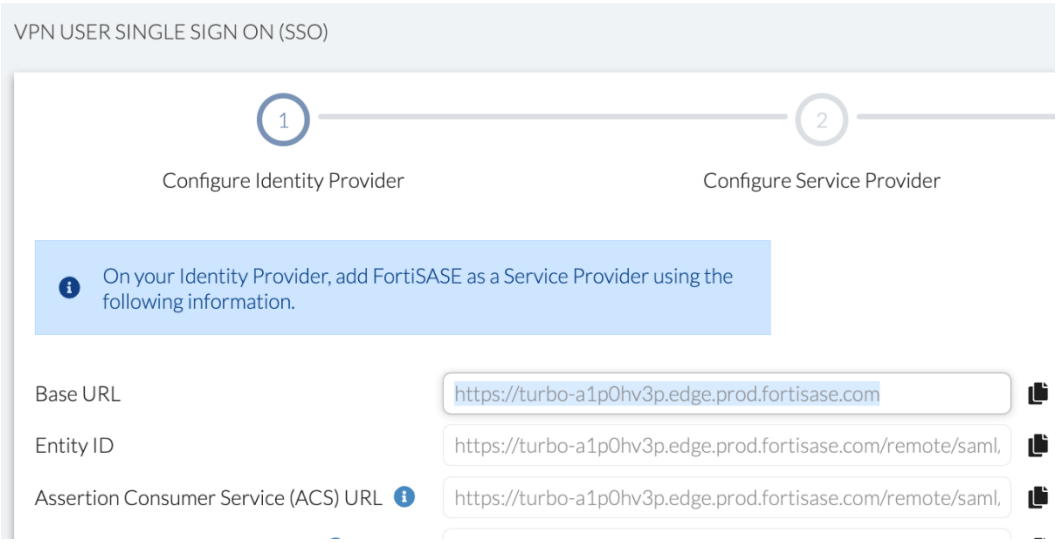
For ease of configuration, following Connecting a FortiAP to FortiSASE using FortiZTP on page 53 is recommended.

As a reference only, this section describes alternative connection methods other than using FortiZTP.

Before using the FortiAP GUI or CLI steps, you must obtain the FortiSASE domain name from FortiSASE.

To obtain the FortiSASE domain name from FortiSASE:

1. Go to *Configuration* > *VPN User SSO*.
2. View the URL in the *Base URL* field and note the FortiSASE domain name after the https:// string. In the example, the FortiSASE domain name is turbo-a1p0hv3p.edge.prod.fortisase.com.



To connect a FortiAP to FortiSASE via the GUI:

1. Log in to the FortiAP GUI.
2. Go to *Settings* > *Local Configuration*.
3. For *AC Discovery Type*, select *DNS*.
4. For *AC Host Name 1*, copy and paste the FortiSASE domain name that you obtained.
5. Click *OK*.

6. If you are using FortiAP Configuration mode, do the following:
   a. To exit this mode, go to the admin menu at the top-right corner and click *Reboot*.
   b. Click *Yes*. Configuration changes take effect after the FortiAP reboots.
7. Connect the FortiAP port to a wired network with internet access. The FortiAP connects to FortiSASE using the domain name configured.

To connect a FortiAP to FortiSASE via the CLI:

1. Connect to FortiAP by starting one of the following:
   a. SSH session with the FortiAP IP address
   b. Console session if your FortiAP has a console port
2. Log in to the FortiAP CLI.
3. Enter these configuration commands:

```
cfg -a AC_DISCOVERY_TYPE=3
cfg -a AC_HOSTNAME_1=<FortiSASE domain name>
cfg -c
```

4. If you are using FortiAP Configuration mode, enter `reboot` to exit this mode. Configuration changes take effect after the FortiAP reboots.
5. Connect the FortiAP port to a wired network with internet access. The FortiAP connects to FortiSASE using the domain name configured.

Upgrading to a supported FortiAP firmware version using alternative connection methods

For ease of configuration, following Authorizing a FortiAP and upgrading to a supported FortiAP firmware version on page 55orUpgrading to the latest supported FortiAP firmware version after authorization on page 57 is recommended.

As a reference only, this section describes FortiAP firmware upgrades using alternative connection methods other than the recommended methods.

If the FortiAP runs an unsupported firmware version, prior to connecting a FortiAP to FortiSASE, you generally must perform these preliminary steps on the FortiAP to ensure proper connectivity:

1. Upgrade the FortiAP to the latest firmware version known to work with FortiSASE using the FortiAP upgrade path. You will save one or more the firmware files locally to your computer and upload the firmware to the device using the FortiAP GUI. See SIA for FortiAP site-based remote users.
2. Factory reset the FortiAP device. For this step, you will use the FortiAP CLI and an SSH client to ensure no prior configuration remains on the device.

To upgrade the FortiAP firmware to the latest version using the FortiAP upgrade path:

1. Connect and log in to the FortiAP GUI as follows:
   a. Connect the FortiAP unit from the LAN 1 port to a separate private switch or hub via a straight-through Ethernet cable or directly connect from the LAN 1 port to your computer Ethernet port via a crossover cable.
   b. Change your computer IP address to 192.168.1.3.
   c. Using a web browser on your computer, connect to https://192.168.1.2. This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.
   d. Log in with the username *admin* and no password.

2. Check the current firmware version on the FortiAP GUI from *Information* > *Dashboard* and in the *Firmware* widget by noting the *Firmware Version* field. Note the four-digit number after build. For example, if you see build0001, 0001 is the build number.
3. Review Supported Upgrade Paths, which lists the FortiAP firmware upgrade path required to upgrade to the supported FortiAP firmware version:
   a. In the *Build #* column, find the build number matching the current firmware version.
   b. In the *Path* column, note the other firmware versions needed. There may be one or more firmware versions required in the upgrade path to upgrade to the supported firmware version. You will need to download the firmware image files for these versions corresponding to your FortiAP device model from the Fortinet Support Site.
4. From the Fortinet Support Site, download the FortiAP firmware image files in the supported upgrade path corresponding to the FortiAP device model, saving them locally to your computer. The firmware image files will be uploaded to the FortiAP device using the FortiAP GUI.
5. From admin dropdown on the top-right, click *Upload/Upgrade*.
6. In the dropdown, select *Image*, click *Image File*, and select the desired firmware image file location saved locally on your computer.
7. Click *Upload* to start the upgrade. You see an *Uploading* dialog as the file upload proceeds. FortiAP reboots automatically to complete the firmware upgrade.
8. Reconnect and log into the FortiAP GUI and confirm the firmware version updated as desired.
9. If necessary, repeat steps 5-8 for each firmware in the supported upgrade path until all the steps in the path are complete.

To factory reset the FortiAP device:

1. Connect the FortiAP unit from the LAN 1 port to a separate private switch or hub via a straight-through Ethernet cable or directly connect from the LAN 1 port to your computer Ethernet port via a cross-over cable.
2. Change your computer IP address to 192.168.1.3.
3. Using an SSH client on your computer, connect to 192.168.1.2 . You may need to download and install an SSH client if it has not been previously installed on your computer.
4. Enter the following FortiAP CLI command to factory reset the device: `factoryreset`
5. Confirm the factory reset when prompted by entering `y`:

```
FortiAP # factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y
```

A reboot occurs as part of the factory reset process.

SD-WAN On-Ramp

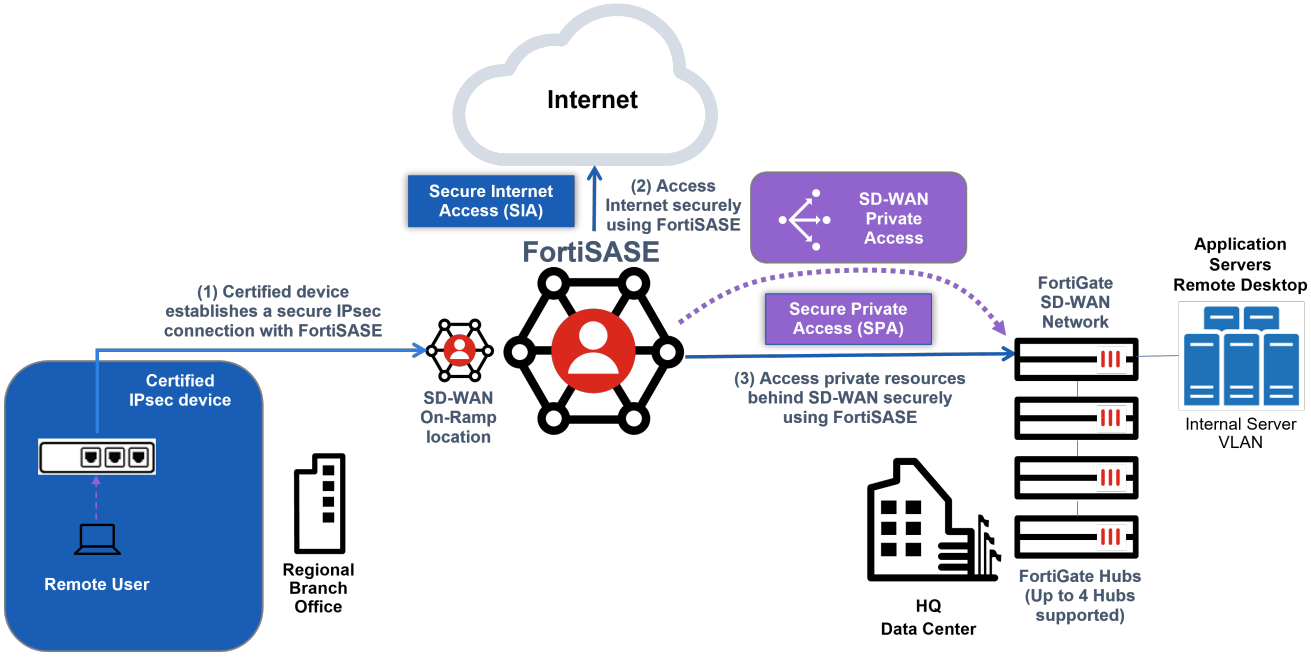
SD-WAN On-Ramp is a select availability feature that requires a FortiSASE instance with an Advanced or a Comprehensive license applied and a separate FortiSASE subscription license per certified IPsec device. This license restricts the number of On-Ramp locations that can be deployed based on the number of seats (2 to 8 seats) specified in the license. Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each certified IPsec device.

Currently, the FortiGate is the only certified IPsec device that can be used for the SD-WAN On-Ramp feature.

You can configure a certified IPsec device for the SD-WAN On-Ramp feature by setting up an IPsec tunnel between the certified IPsec device and a FortiSASE SD-WAN On-Ramp location. In this use case, because the certified IPsec device is responsible for centralizing its remote users' site connectivity to the FortiSASE firewall-as-a-service (FWaaS), the endpoints only need to be configured in their IP settings to forward traffic to the FortiGate as the default gateway.

Multiple branch devices can establish IPsec connections with the SD-WAN On-Ramp location.

Therefore, for this use case, individual workstation or device setup is minimized because FortiClient does not need to be installed on endpoints and web browser-based endpoints do not require explicit web proxy settings to be configured.



BGP configuration is shared between the SD-WAN On-Ramp and Secure Private Access (SPA) features. You must configure the SPA network configuration first before deploying an SD-WAN On-Ramp location but SPA service connections can be created after deploying an SD-WAN On-Ramp location.

When deep inspection is enabled, to avoid certificate errors and ensure proper inspection of encrypted traffic by FortiSASE security features, the FortiSASE CA certificate must be manually installed on endpoints for agentless SWG users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Prerequisites

SD-WAN On-Ramp is a select availability feature that requires a FortiSASE instance with an Advanced or a Comprehensive license applied and a separate FortiSASE subscription license per certified IPsec device. This license restricts the number of On-Ramp locations that can be deployed based on the number of seats (2 to 8 seats) specified in the license. Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each certified IPsec device.

Currently, the FortiGate is the only certified IPsec device that can be used for the SD-WAN On-Ramp feature.

BGP configuration is shared between the SD-WAN On-Ramp and Secure Private Access (SPA) features. You must configure the SPA network configuration first before deploying an SD-WAN On-Ramp location but SPA service connections can be created after deploying an SD-WAN On-Ramp location.

Supported models and firmware

For a list of model and firmware version prerequisites, see SIA for SD-WAN On-Ramp site-based remote users.

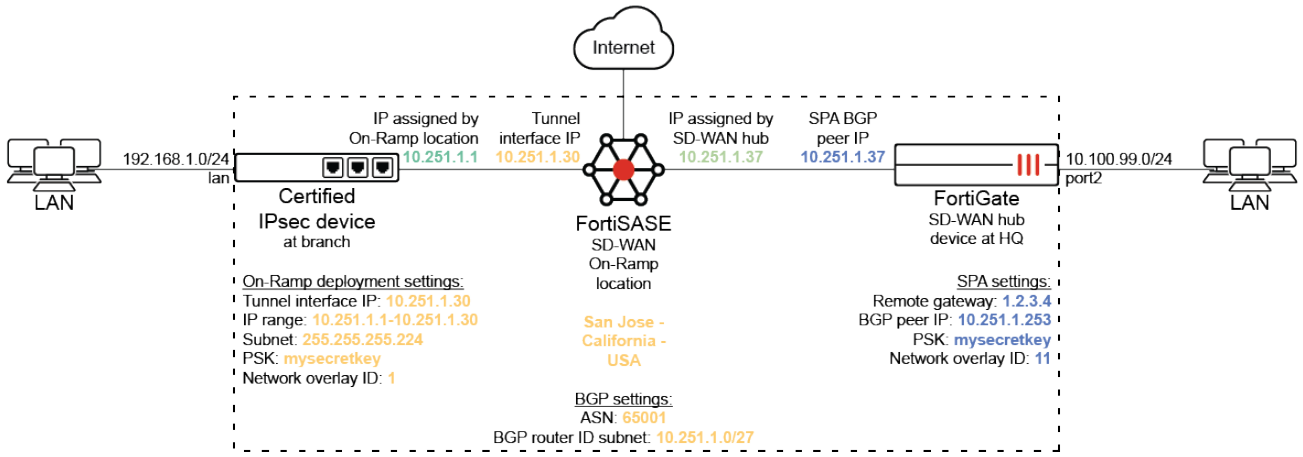
FortiCloud account prerequisites

To activate SD-WAN On-Ramp management support on FortiSASE, you must purchase and apply a FortiSASE subscription license to your instance. You can enable connectivity from different IPsec device types as part of the same license. See SIA for SD-WAN On-Ramp site-based remote users or the SASE and Zero Trust Ordering Guide.

For details on registering products, see Registering assets.

Network topology

The following diagram depicts an example network topology that a certified IPsec device uses for FortiSASE SD-WAN On-Ramp:



An IPsec VPN tunnel is established between the certified IPsec device and a FortiSASE SD-WAN On-Ramp location.

Multiple branch devices can establish IPsec connections with the SD-WAN On-Ramp location.

The example network topology uses the following settings configured in FortiSASE:

Configuration setting	Value used in example network topology
On-Ramp deployment settings	
Tunnel Interface IP	10.251.1.30
IP range	10.251.1.1-10.251.1.30
Subnet	255.255.255.224
Pre-shared key	mysecretkey
Secure private access settings	
Remote gateway	1.2.3.4
BGP Peer IP	10.251.1.253
Pre-shared key	mysecretkey
Network Overlay ID	11

SSL deep inspection for site-based users

When you enable deep inspection, to avoid certificate errors and ensure FortiSASE security features properly inspect encrypted traffic, you must manually install the FortiSASE certificate authority certificate on endpoints for agentless secure web gateway users and site-based edge device users. See Installing a certificate for deep inspection mode on page 148.

Configuring IPsec device as SD-WAN On-Ramp

The FortiGate is the only certified IPsec device that you can use for SD-WAN On-Ramp.

The SD-WAN On-Ramp and secure private access (SPA) features share BGP configuration. You must configure the SPA network configuration first before deploying an SD-WAN On-Ramp location but you can create SPA service connections after deploying an SD-WAN On-Ramp location.

In *Edge Devices* > *SD-WAN On-Ramp*, you can configure certified IPsec devices:

- Configuring BGP on page 69
- Configuring On-Ramp locations on page 70

Configuring BGP

BGP configuration is shared between the SD-WAN On-Ramp and Secure Private Access (SPA) features. You must configure the SPA network configuration first before deploying an SD-WAN On-Ramp location but SPA service connections can be created after deploying an SD-WAN On-Ramp location.

To configure BGP settings for SD-WAN On-Ramp:

1. Go to *Edge Devices* > *SD-WAN On-Ramp*.
2. Click the *BGP* tab.

3. Configure the following BGP settings:

Network attributes	Description	Example
BGP router ID subnet	Available/unused subnet that can be used to assign loopback interface IP addresses used for BGP router IDs parameter on the FortiSASE SD-WAN On-Ramp location. /28 is the minimum subnet size. Typically, this BGP router ID subnet is a subnet within the overall BGP loopback summary range that is currently unused. For example, if the BGP loopback summary range is 10.251.1.0/24 then you can choose to configure 10.251.1.0/27 as the BGP router ID subnet. For BGP on loopback, you must configure this subnet as a neighbor range in the hub BGP settings.	10.251.1.0/27
Autonomous system number (ASN)	BGP autonomous system (AS) number used by the IPsec device and FortiSASE. Since FortiSASE supports iBGP, the IPsec branch device must be configured with the BGP ASN configured in this field. Also, if the SPA feature is configured in FortiSASE, the BGP ASN in this field must also match the value defined in the SPA network configuration page.	65001

4. Click *OK*.

Configuring On-Ramp locations

SD-WAN On-Ramp is a select availability feature that requires a FortiSASE instance with an Advanced or a Comprehensive license applied and a separate FortiSASE subscription license per certified IPsec device. This license restricts the number of On-Ramp locations that can be deployed based on the number of seats (2 to 8 seats) specified in the license. Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each certified IPsec device.

Currently, the FortiGate is the only certified IPsec device that can be used for the SD-WAN On-Ramp feature.

BGP configuration is shared between the SD-WAN On-Ramp and Secure Private Access (SPA) features. You must configure the SPA network configuration first before deploying an SD-WAN On-Ramp location but SPA service connections can be created after deploying an SD-WAN On-Ramp location.

To configure deploy an SD-WAN On-Ramp location:

1. Go to *Edge Devices* > *SD-WAN On-Ramp*.
2. Click the *On-Ramp locations* tab.
3. Click + *Deploy On-Ramp location*.

4. Configure the following settings in the *Deploy On-Ramp Location* page:

Setting	Description	Example
On-Ramp location		
Location	The datacenter to be deployed as an SD-WAN On-Ramp location.	San Jose - California -USA
IPsec tunnel		
Tunnel interface IP	The IP address defined on the IPsec tunnel interface for the SD-WAN On-Ramp location.	10.251.1.30
IP range	The IP address range used by the SD-WAN On-Ramp location for assigning tunnel interface IP addresses for IPsec devices using mode configuration.	10.251.1.1-10.251.1.30
Subnet mask	The subnet mask corresponding to the IP range used by the SD-WAN On-Ramp location for IP assignment.	255.255.255.224
Pre-shared Key	The IPsec device authenticates with the SD-WAN On-Ramp location using the Pre-shared key authentication method. Define the pre-shared key.	mysecretkey

5. Click *OK*.
6. In the *On-Ramp locations* page, observe the *Status* begins as *Pending*, the *FQDN* field with a corresponding value, and the *Tunnel interface IP* defined as configured in previous steps. Once the SD-WAN On-Ramp location has been successfully deployed, *Status* changes to *Running*.
7. Take note of the *FQDN* field and *Tunnel interface IP* which will be used for IPsec device configuration.

Configuring a FortiGate IPsec connection to FortiSASE

Currently, the FortiGate is the only certified IPsec device that can be used for the SD-WAN On-Ramp feature.

After deploying an SD-WAN On-Ramp location in FortiSASE, you can configure the FortiGate as a certified IPsec device to establish an IPsec connection to FortiSASE:

- Connecting and logging into the FortiGate
- IPsec VPN configuration using IPsec wizard and CLI
- BGP configuration
- Verifying and troubleshooting the IPsec VPN connection
- Verifying and troubleshooting BGP and static routing

Connect and logging into the FortiGate

For details on connecting and logging into the FortiGate GUI, see Connecting using a web browser.

For details on connecting and logging into the FortiGate CLI, see Connecting to the CLI.

IPsec VPN configuration using IPsec wizard and CLI

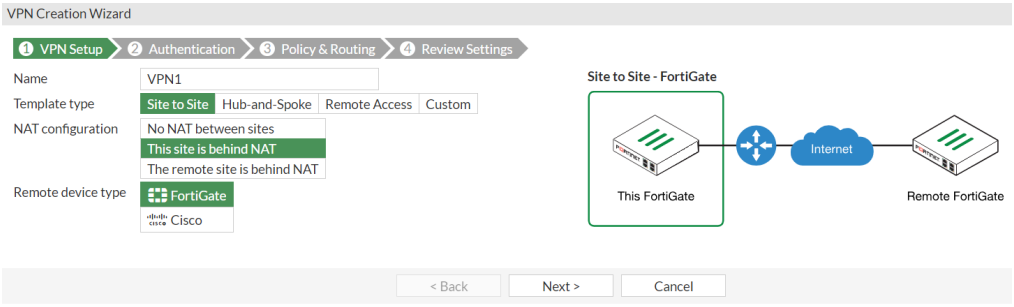
The FortiGate as an IPsec device for SD-WAN On-Ramp requires the following IPsec VPN settings:

- IKEv2
- Branch device configured as an IPsec VPN dialup client. Your branch device connects to the FortiSASE SD-WAN On-Ramp location, which acts as a remote site.
- You must enable the mode config setting. Each FortiSASE SD-WAN On-Ramp location assigns IP addresses, and the branch device automatically configures its tunnel interfaces IP address with the acquired IP address. You also use this IP address to set up BGP peering.
- On branches, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
  Use network overlay IDs for each overlay tunnel configuring set network-overlay enable and set network-id <n>
  Branch devices must be configured with a network ID of 1.
- Pre-shared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, only aes256-sha256 is supported.
  - For IPsec phase 2, only aes256-sha256 is supported.

The following settings are only examples. Do not consider them as recommended settings.

To configure an IPsec VPN using the GUI and IPsec wizard:

1. On the FortiGate, go to *VPN* > *IPsec Wizard*. The *VPN Creation Wizard* displays.
2. Configure the following *VPN Setup* options:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Site to Site*.
   c. For *NAT configuration*, select the option that corresponds to your network topology.
   d. For *Remote device type*, select *FortiGate*.
   e. Click *Next*.



3. Configure the following *Authentication* options:
   a. For *Remote device*, select *Dynamic DNS*.
   b. For *FQDN*, paste the *FQDN* from the *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* page. Notice that the FortiGate displays *Resolved to* < *IP address* >. Make note of this IP address since it will be used later.
   c. From the *Outgoing Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections. For example, you could select *wan1*.

   d. For *Authentication method*, select *Pre-shared Key*.
   e. In the *Pre-shared key* field, enter the desired key in alphanumeric characters. Click *Next*.
4. Configure the following *Tunnel Interface* options:
   a. In the *Tunnel IP* field, enter 10.251.1.1.
   b. In the *Remote IP/netmask* field, enter 10.251.1.30/32. Click *Next*.
      The tunnel interface IP address is assigned by mode configuration. However, this step simply configures placeholder values to allow the IPsec wizard to proceed.
5. Configure the following *Policy & Routing* options:
   a. Set *Local interface* to the desired LAN interface(s).
   b. Observe that the *Local subnets* are automatically detected based on the LAN interface(s) selected.
   c. For *Remote Subnets* since there are no specific destinations, enter 0.0.0.0/0
   d. For *Internet access*, select *None*. Click *Next*.
6. Configure the following settings using the CLI. The IPsec wizard does not configure these settings. Replace VPN1 with your actual IPsec VPN phase 1 name:
   a. Enable IKEv2
   b. Enable network overlays
   c. Set the VPN gateway network ID to 1.
   d. Enable mode config.

```
config vpn ipsec phase2-interface
   delete VPN1
end
config vpn ipsec phase1-interface
   edit VPN1
      set ike-version 2
      set network-overlay enable
      set network-id 1
      set mode-cfg enable
      set auto-discovery-receiver enable
   next
end
config vpn ipsec phase2-interface
   edit "VPN1"
      set phase1name "VPN1"
      set proposal aes256-sha256
   next
end
```

BGP, SD-WAN, and routing configuration

Once the IPsec tunnel has been established, you must configure routing settings on the branch FortiGate to ensure the following operation:

1. Ensuring access to local subnets to FortiSASE for secure Internet access reply traffic
2. Outgoing routing to FortiSASE for secure Internet access
3. Outgoing routing to WAN connection for direct Internet access, if applicable

You can use iBGP or static routing with source NAT to achieve the first objective. You can use static routing alone or static routing with SD-WAN for traffic steering to achieve the second and third objective.

This topic covers the following:

BGP configuration considerations

The branch FortiGate connects to the FortiSASE SD-WAN On-Ramp location and establishes an iBGP peering with it. Using iBGP, the FortiSASE SD-WAN On-Ramp location can learn routes to your network.

The branch FortiGate requires the following BGP settings:

- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for SD-WAN On-Ramp location
- One BGP session per overlay between the branch and the SD-WAN On-Ramp location

This section describes BGP settings that you must configure since the IPsec wizard creates does not include them.

The FortiSASE SD-WAN On-Ramp feature supports the routing design using iBGP to learn routes to your local networks behind the branch FortiGate. With this routing design, the On-Ramp location can see the source IP address of the client connected behind the IPsec device.

If you decide to use static routing on the branch FortiGate for your routing design, then you must configure source NAT on the branch FortiGate firewall policy destined for the On-Ramp location for reply traffic from the On-Ramp location to be routed back to the branch FortiGate. With this routing design, the On-Ramp location only sees the tunnel interface IP address of the FortiGate IPsec device and not the source IP address of the client connected behind the IPsec device.

Static routing and SD-WAN configuration considerations

The administrative distance of the static route using the IPsec tunnel interface varies depending on how IPsec was configured on the branch FortiGate:

- When using the IPsec wizard on the branch FortiGate, a static route to the peer local subnet, 0.0.0.0/0 in the example configuration used previously, using the IPsec tunnel interface is created with a default administrative distance of 10.
- If you configure IPsec on the branch FortiGate as a Custom tunnel, then with *set add-route enable* by default, FortiGate dynamic IPsec route control will add a static route to peer destination selector with a default administrative distance of 15. If the peer destination selector is set to 0.0.0.0/0 then the default static route has an administrative distance of 15.

For routing configuration on the branch FortiGate, you have the following options for routing traffic through the IPsec tunnel acting as a full tunnel to the SD-WAN On-Ramp location:

1. Configure the existing default route using the WAN interface to have the same administrative distance as the default route using the IPsec tunnel interface. Then configure SD-WAN for traffic steering.
2. Configure the existing default route using the WAN interface to have a greater distance (making this the less preferred route) than the static route using the IPsec tunnel interface and just leverage this latter route.

When configuring the static default route for full tunneling above, connected routes for locally connected subnets will be included in the FortiGate routing table. A local DNS server that is directly connected to one of these subnets would be accessible without further configuration.

However, if your branch device is using a local DNS server that is on a subnet different than a local interface, then you must configure a new static route for that DNS server to ensure that DNS traffic does not mistakenly route to FortiSASE instead.

In this topic we give an example of static routing with SD-WAN for traffic steering.

BGP configuration

To configure BGP using the GUI:

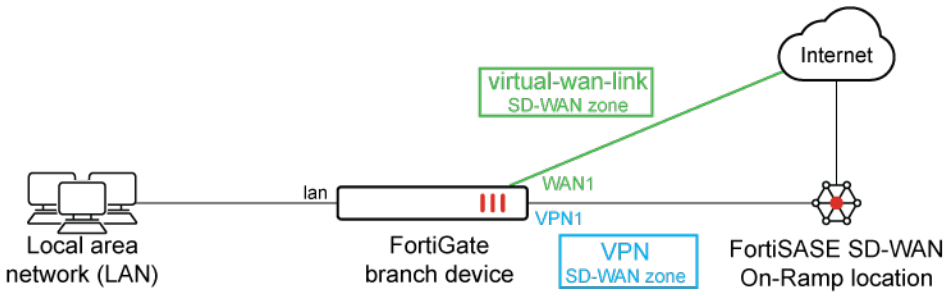
If you cannot view the *Network* > *BGP* tree menu, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.

1. On the FortiGate, go to *Network* > *BGP*.
2. Confirm that the *Local AS* field is set to 65001.
3. In the *Router ID* field, enter 10.251.1.1, which corresponds to the tunnel interface IP assigned by the SD-WAN On-Ramp location via mode configuration.
4. Under *Neighbors*, click + *Create New*.
   a. For *IP*, enter *Tunnel interface IP* from the *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* page.
   b. For *Remote AS*, enter 65001.
   c. In the options, enable *Soft reconfiguration* and *Capability: route refresh*.
   d. Click *OK*.
5. Under *Networks*, add the LAN subnets in the *IP/Netmask* field. Click + to add more subnets, if necessary.
6. Click *Apply*.

Static routing with SD-WAN configuration

The following network topology and configuration provide a basic SD-WAN example applied to branch FortiGate use cases for direct Internet access and secure Internet access with FortiSASE. For further details and other use cases, see SD-WAN quick start, SD-WAN members and zones, Performance SLA, and SD-WAN rules.

The following network topology is used for the static routing and SD-WAN configuration:



For this topology, we have a single underlay interface *WAN1* and single overlay interface *VPN1*, and corresponding *virtual-wan-link* and *VPN* SD-WAN zones, respectively. The *virtual-wan-link* SD-WAN zone is used for direct Internet access for critical, latency-sensitive traffic that bypasses FortiSASE and the VPN SD-WAN zone is used for secure Internet access through FortiSASE. In example, traffic to example.com is considered critical and latency sensitive.

To configure static routing in preparation for SD-WAN:

1. On the FortiGate, go to *Network* > *Static Routes*.
2. Click to select the route with the *Destination* of *0.0.0.0/0* and *Interface* set to the WAN interface.
3. Click *Edit in CLI*.
   a. If the IPsec wizard was previously used, enter these CLI commands to configure distance equal to the static route created by the wizard (note that this step can be skipped if a default static route was manually created for the WAN interface previously since static routes default to a distance of 10):

   ```
   set distance 10
   show
   end
   ```

   b. If the IPsec Custom tunnel option was used, enter these CLI commands to configure distance equal to the static route added by dynamic IP route control:

   ```
   set distance 15
   show
   end
   ```

4. Go to *Dashboard* > *Network* and in the *Routing* widget click *Expand* to full screen. By default, the *Static & Dynamic* view should be selected from the dropdown at the top-right.
5. Confirm that both the route for the WAN interface and the route for the IPsec tunnel interface as visible as two separate entries in the routing table:

   Route for WAN interface:

Field	Value
Network	0.0.0.0/0
Gateway IP	<Default gateway corresponding to WAN interface>
Interfaces	<Name of WAN interface>
Distance	10 if IPsec wizard previously used 15 if IPsec Custom tunnel previously used
Type	Static

   Route for IPsec tunnel interface:

Field	Value
Network	0.0.0.0/0
Gateway IP	<Blank>
Interfaces	<Name of IPsec tunnel interface>
Distance	10 if IPsec wizard previously used

Field	Value
	15 if IPsec Custom tunnel previously used
Type	Static

To configure SD-WAN for traffic steering:

1. On the FortiGate, go to *Policy & Objects* > *Firewall Policy*.
2. Select any firewall policies where the WAN or IPsec tunnel interfaces are either configured as source or destination interfaces by holding CTRL and clicking on policies. Click on Delete to delete them. This is required to select these interfaces as SD-WAN members.
3. Create a new VPN zone and assign member interfaces to SD-WAN zones.
   a. Go to *Network* > *SD-WAN* and select the *SD-WAN Zones* tab.
   b. Select *virtual-wan-link* and click *Edit*.
      i. Set the *Interface members* to *wan1*.
      ii. Click *OK*.
   c. Click *Create New* > *SD-WAN Zone*.
      i. Enter the *Name* as *VPN*.
      ii. Set the *Interface members* to *VPN1*.
      iii. Click *OK*.
4. Create a new performance SLA to detect latency.
   a. Go to *Network* > *SD-WAN* and select the *Performance SLAs* tab.
   b. Click *Create New*.
   c. In the *New Performance SLA* page, enter these values (leave unspecified values to default values):

Field	Value
Name	Internet
Probe mode	Active
Protocol	Ping
Server	8.8.8.8
Participants	1. Click *Specify*. 2. Select *VPN1*, then *wan1*, and click *Close*.
SLA Target	Enabled
Latency threshold	Enabled Set to 170 ms.
Jitter threshold	Disabled
Packet loss threshold	Disabled

   d. Click *OK*.
5. Create an SD-WAN rule for critical direct Internet access traffic only. In this example, any traffic to example.com will bypass FortiSASE and will use the branch FortiGate WAN interface directly.

a. Go to *Network* > *SD-WAN* and select the *SD-WAN Rules* tab.
b. Click *Create new*.
c. In the *Priority Rule* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Critical-DIA
Status	Enabled
Source	
Address	all
Destination	
Address	1. Click on +. 2. Click *+Create*. 3. Click *+Firewall Address*. 4. Create a *New Address*. 5. Set the *Name* as *example.com*. 6. Set the *Type* as *FQDN*. 7. Set *FQDN* as *example.com*. 8. Set the *Interface* as *any*. 9. Set the *Static route configuration* as *Disabled*. 10. Click *OK*. 11. The newly created FQDN should be selected. Click *Close*.
Protocol number	ANY
Interface selection strategy	Lowest cost (SLA)
Interface preference	1. Select *wan1* and then *VPN1*. 2. Click *Close*.
Required SLA target	Internet#1

d. Click *OK*.

6. Create an SD-WAN rule low priority secure Internet access traffic only.
a. Go to *Network* > *SD-WAN* and select the *SD-WAN Rules* tab.
b. Click *Create new*.

c. In the *Priority Rule* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Low-Priority-SIA
Status	Enabled
Source	
Address	all
Destination	
Address	all
Protocol number	ANY
Interface selection strategy	Lowest cost (SLA)
Interface preference	1. Select *wan1* and then *VPN1*. 2. Click *Close*.
Required SLA target	Internet#1

d. Click *OK*.

7. Create a firewall policy to allow direct Internet access traffic:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create new*.
   c. In the *New Policy* page, enter the following values. Leave unspecified values to default values.

Field	Value
Name	Direct Internet Access
Incoming Interface	lan
Outgoing Interface	virtual-wan-link
Source	all
Destination	all
Service	ALL
NAT	Enabled
IP Pool Configuration	Use Outgoing Interface Address
Log Allowed Traffic	Enabled Select *All Sessions*.

   d. Click *OK*.
8. Create a firewall policy to allow secure Internet access traffic:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create new*.

c. In the *New Policy* page, enter the following values. Leave unspecified values to default values.

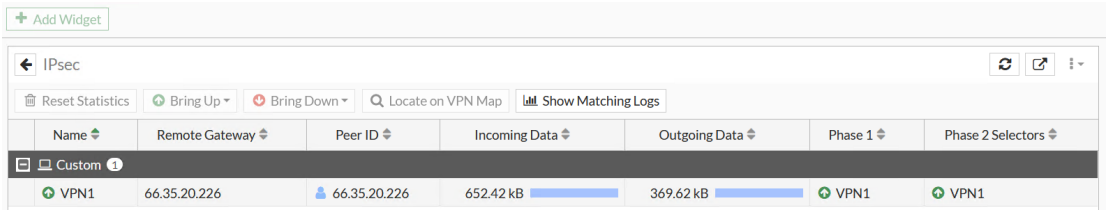
Field	Value
Name	Secure Internet Access
Incoming Interface	lan
Outgoing Interface	VPN
Source	all
Destination	all
Service	ALL
NAT	Disabled
Log Allowed Traffic	Enabled Select *All Sessions*.

d. Click *OK*.

Verifying and troubleshooting IPsec VPN connection

To verify the IPsec VPN tunnel on a branch FortiGate:

1. Go to *Dashboard* > *Network* and click the *IPsec* widget to expand it.
2. Verify the IPsec tunnel that is established with the SD-WAN On-Ramp location.



To verify Internet traffic is forwarded to FortiSASE:

1. In the FortiGate CLI, check the Public/WAN IP address:

```
Branch1 # diag sys waninfo ipify
Try to get my public IP through https://api.ipify.org with src_ip=0.0.0.0
device=unspecified vfid=0(root) ...

Public/WAN IP: 66.35.20.126
...
```

2. In FortiSASE, go to *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* and copy the FQDN for the On-Ramp location.
3. Confirm that the Public/WAN IP address corresponds to the FortiSASE SD-WAN On-Ramp location by pinging the FQDN used for the On-Ramp location on the FortiGate:

```
Branch1 # exec ping ipsec-be68qi9e-sjc-f1.stage.fortisase.com
PING ipsec-be68qi9e-sjc-f1.stage.fortisase.com (66.35.20.226): 56 data bytes
64 bytes from 66.35.20.126: icmp_seq=0 ttl=243 time=23.2 ms
64 bytes from 66.35.20.126: icmp_seq=1 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=2 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=3 ttl=243 time=22.6 ms
64 bytes from 66.35.20.126: icmp_seq=4 ttl=243 time=22.5 ms

--- ipsec-be68qi9e-sjc-f1.stage.fortisase.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 22.5/22.7/23.2 ms
```

To troubleshoot the IPsec VPN tunnel on a branch FortiGate:

If after configuring the FortiGate, the IPsec VPN tunnel is not established, then perform the following troubleshooting steps.

1. On the branch FortiGate, run this CLI command to ensure the SD-WAN On-Ramp location FQDN is responding to pings:
   ```
   exec ping <FQDN>
   ```
   If these pings time out, then ensure that the On-Ramp location in *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* has a *Status* of *Running*.

   If the *Status* says *Running* and you just finished deploying the On-Ramp location, then you may need to wait a few minutes before the FQDN responds to pings.
2. On the branch FortiGate, run these CLI commands to capture IKE debug messages:

   ```
   diag debug console timestamp enable
   diag debug application ike -1
   diag debug enable
   ```

   Wait for a few messages to be displayed then disable them by running this command:

   ```
   diag debug disable
   ```

   If you see these error messages:

   ```
   ike 0:VPN1:765: negotiation timeout, deleting
   ike 0:VPN1: connection expiring due to phase1 down
   ike 0:VPN1: deleting
   ```

   Verify the IPsec VPN Phase 1 configuration settings are correct on the branch FortiGate from the GUI:
   a. Go to *VPN* > *IPsec Tunnels*.
   b. Select the tunnel and click *Edit*.
   c. Click *Convert To Custom Tunnel*.
   d. Verify the following settings match with the deployed SD-WAN On-Ramp location:
      i. In *Network*, ensure the *Dynamic DNS* field has the correct FQDN from the *Edge Devices* > *SD-WAN On-Ramp* > *On-Ramp locations* page.
      ii. In *IKE*, ensure *Version* is set to *2*.
      iii. In *Authentication*, ensure the *Pre-shared Key* has the correct value. Since you cannot view the *Pre-shared Key* value in plaintext, you may need to re-enter this value.
   e. In the CLI, run this command:

      ```
      show vpn ipsec phase1-interface
      ```

Ensure these CLI commands are configured:

```
set network-overlay enable
set network-id 1
```

Verifying and troubleshooting BGP and static routing with SD-WAN

To verify BGP routing on a branch FortiGate:

1. In the CLI, check the BGP peering status:

```
Branch1 # get router info bgp summary

VRF 0 BGP router identifier 10.251.1.1, local AS number 65001
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.251.1.30 4      65001     731     758        1    0    0 00:35:00        0

Total number of neighbors 1
```

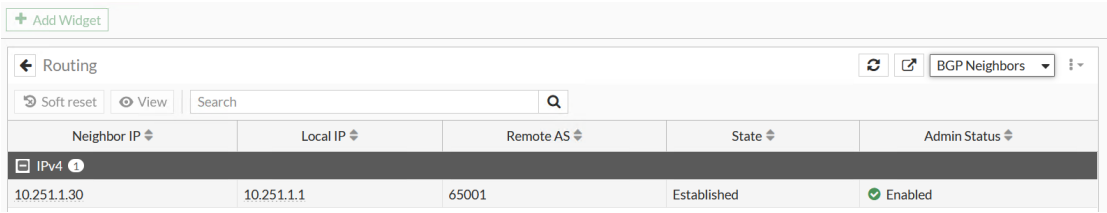
2. Check the BGP advertised routes:

```
Branch1 # get router info bgp neighbor 10.251.1.30 advertised-routes
VRF 0 BGP table version is 1, local router ID is 10.251.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i192.168.1.0      10.251.1.1                        100  32768        0 i <-/->

Total number of prefixes 1
```

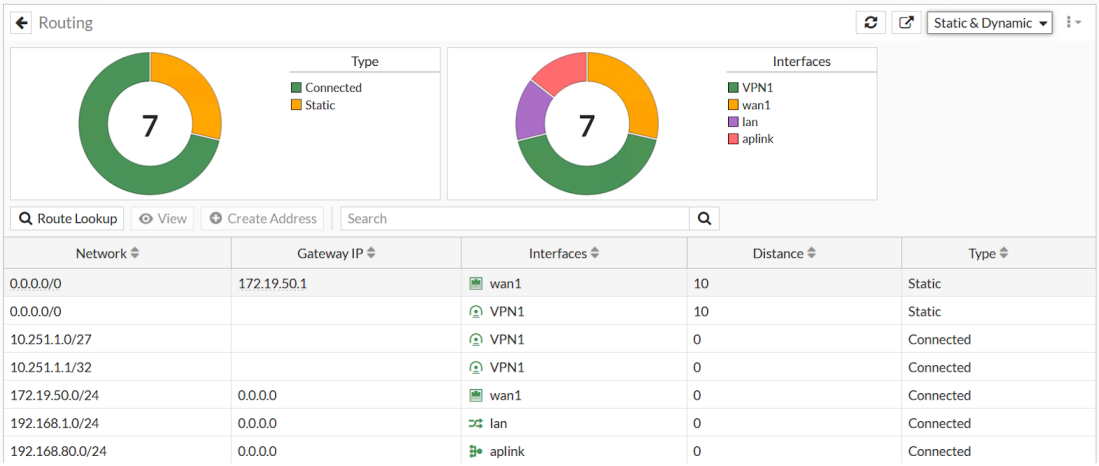
3. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
4. In the dropdown, select *BGP Neighbors*.



To verify static routing with SD-WAN on a branch FortiGate:

1. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
2. In the dropdown, select *Static & Dynamic*.
3. Observe that default static routes to wan1 and VPN1 interfaces have the same distance and both exist in the routing

table.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	172.19.50.1	wan1	10	Static
0.0.0.0/0		VPN1	10	Static
10.251.1.0/27		VPN1	0	Connected
10.251.1.1/32		VPN1	0	Connected
172.19.50.0/24	0.0.0.0	wan1	0	Connected
192.168.1.0/24	0.0.0.0	lan	0	Connected
192.168.80.0/24	0.0.0.0	aplink	0	Connected

To verify SD-WAN on a branch FortiGate using a client computer:

1. On a client computer, enter the following in a Windows Command Prompt:

```
C:\> ping example.com

Pinging example.com [93.184.215.14] with 32 bytes of data:
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55
Reply from 93.184.215.14: bytes=32 time=20ms TTL=55
Reply from 93.184.215.14: bytes=32 time=4ms TTL=55

Ping statistics for 93.184.215.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 20ms, Average = 8ms
```

2. On the branch FortiGate, go to *Log & Report* > *Forward Traffic* and confirm the ping traffic for example.com goes through the *Direct Internet Access* policy.
3. On a client computer, enter the following in a Windows Command Prompt:

```
C:\> ping google.com

Pinging google.com [142.250.191.46] with 32 bytes of data:
Reply from 142.250.191.46: bytes=32 time=25ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113
Reply from 142.250.191.46: bytes=32 time=24ms TTL=113

Ping statistics for 142.250.191.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms
```

4. On the branch FortiGate, go to *Log & Report* > *Forward Traffic* and confirm the ping traffic for google.com goes through the *Secure Internet Access* policy.

To troubleshoot BGP routing on a branch FortiGate:

If after configuring the FortiGate, the BGP peering is not established, perform the following troubleshooting steps.

1. In the CLI, check the BGP peering status:

   ```
   get router info bgp summary
   ```

   If the command returns empty, then confirm these BGP settings from *Network* > *BGP* as correctly configured:
   a. *Local AS*
   b. *Router ID*
   c. *Neighbor*
      i. *IP*
      ii. *Remote AS*
2. Check the BGP advertised routes:

   ```
   get router info bgp neighbor <neighbor IP> advertised-routes
   ```

   If the command returns empty, then confirm from *Network* > *BGP* that the branch FortiGate LAN subnet is configured in Networks with the correct *IP/Netmask*.

To troubleshoot static routing with SD-WAN on a branch FortiGate:

If after configuring the FortiGate, the full tunnel operation is not occurring because of an issue with static routing, then perform the following troubleshooting steps.

Check the current static routes on the branch FortiGate:

1. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
2. In the dropdown, select *Static & Dynamic*.
3. Confirm that the following routes display:
   - Default static route through the VPN tunnel:
     - *Network*: 0.0.0.0
     - *Interface*: <Tunnel interface>
   - Default static route through WAN interface:
     - *Network*: 0.0.0.0
     - *Interface*: < WAN interface >
4. If these routes are not displayed, then carefully review the steps in To configure static routing in preparation for SD-WAN: on page 76.
5. If these routes are displayed, then carefully review the steps in To configure SD-WAN for traffic steering: on page 77.

Viewing IPsec connections

In *Edge Devices* > *SD-WAN On-Ramp*, in the *IPsec connections* tab, you can monitor the IPsec connections established between the IPsec devices and the deployed SD-WAN On-Ramp locations.

Configuring profile groups and policies to control traffic flow from branch devices

After a branch device has been configured with the SD-WAN On-Ramp location, in FortiSASE you can configure profile groups with security features enabled, hosts, and policies to control traffic flow as desired.

For example, the following devices can establish IPsec connections with a deployed SD-WAN On-Ramp location:

- Branch 1 FortiGate with a local subnet of 192.168.1.0/24
- Branch 2 FortiGate with a local subnet of 192.168.10.0/24

In FortiSASE, you can configure the following:

1. Create profile groups and configure security features and settings in *Configuration* > *Security* that are specific to each branch device.
2. Configure hosts in *Configuration* > *Hosts*, namely, IPv4 hosts of the *Subnet* type for each local subnet.
3. Configure a policy for each branch with these settings:
   a. *Source Scope*: *Edge Device*
   b. *Source*: Specify and select the host created for the branch local subnet
   c. *Action*: *Accept*
   d. *Profile Group*: Specify and select the profile group created for the branch

You can confirm policies for *Internet Access* and *Private Access*, as desired.

See Security profile groups on page 145 and Configuring a policy to allow traffic from an Edge device to FortiSASE on page 141.

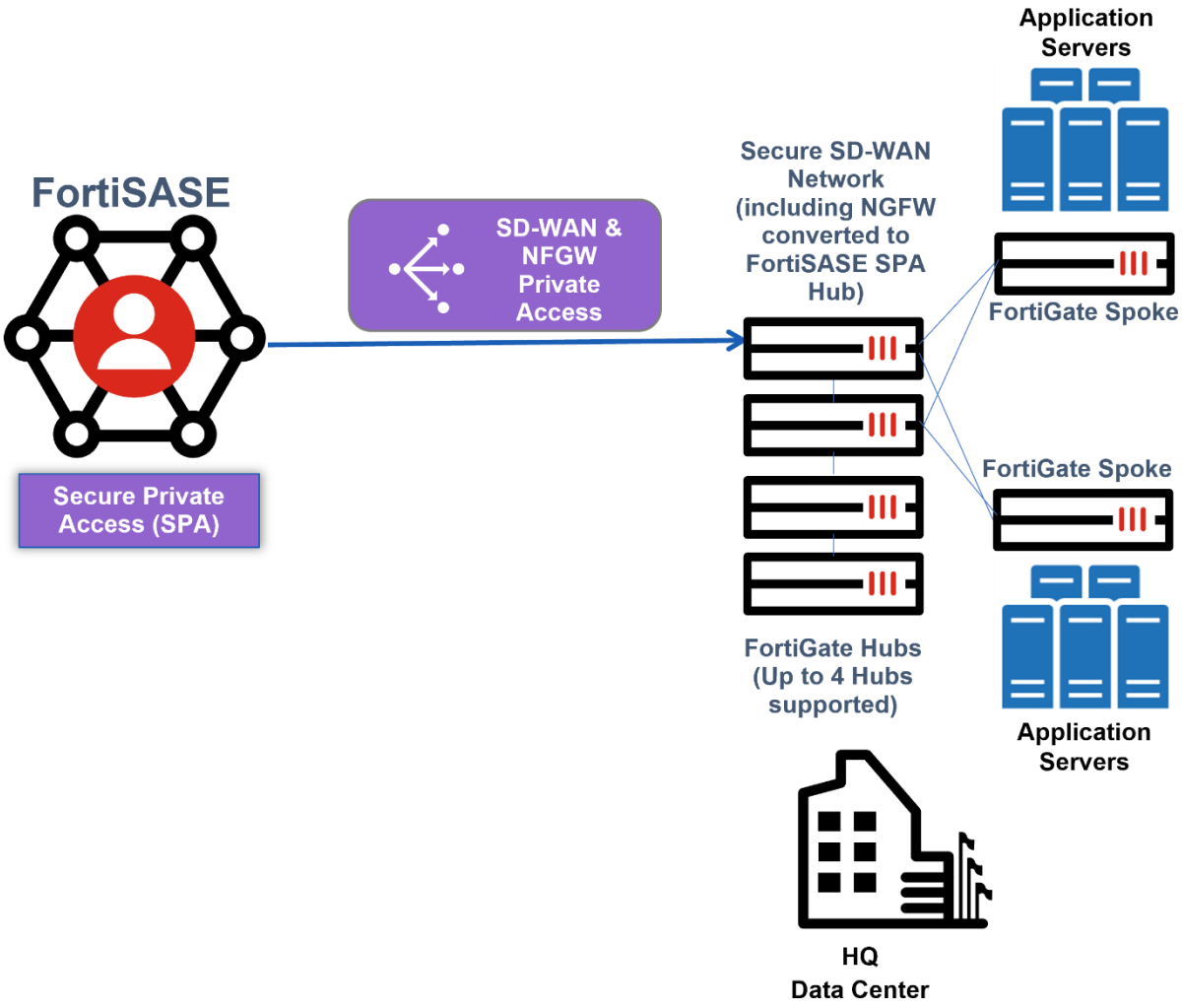
Network

FortiSASE includes the following so that you can easily monitor your network:

Dashboard	Description
Asset Map	Displays on a global map the geographical location of assets, including security PoPs, private access hubs, edge devices (FortiAP, FortiExtender, FortiGate), and endpoints (hidden by default). For a security PoP, indicates status, number of connected units, and logging support (if enabled). For larger topologies, groups multiple asset types and single asset types for global, regional, and local views using number bubbles.
Secure Private Access	Add, delete, and update common secure private access (SPA) network configuration and add, delete, update, and monitor SPA service connections to FortiGate SPA hub.
Managed Endpoints	View and deregister endpoints that FortiSASE is managing.
Connected Users	View and deauthenticate users that are connected to FortiSASE.
Digital Experience Monitoring	View health check metrics for digital experience monitoring (DEM) of first-mile connectivity between SaaS applications and each of the geographical points of presence (PoPs) provisioned for your FortiSASE instance.

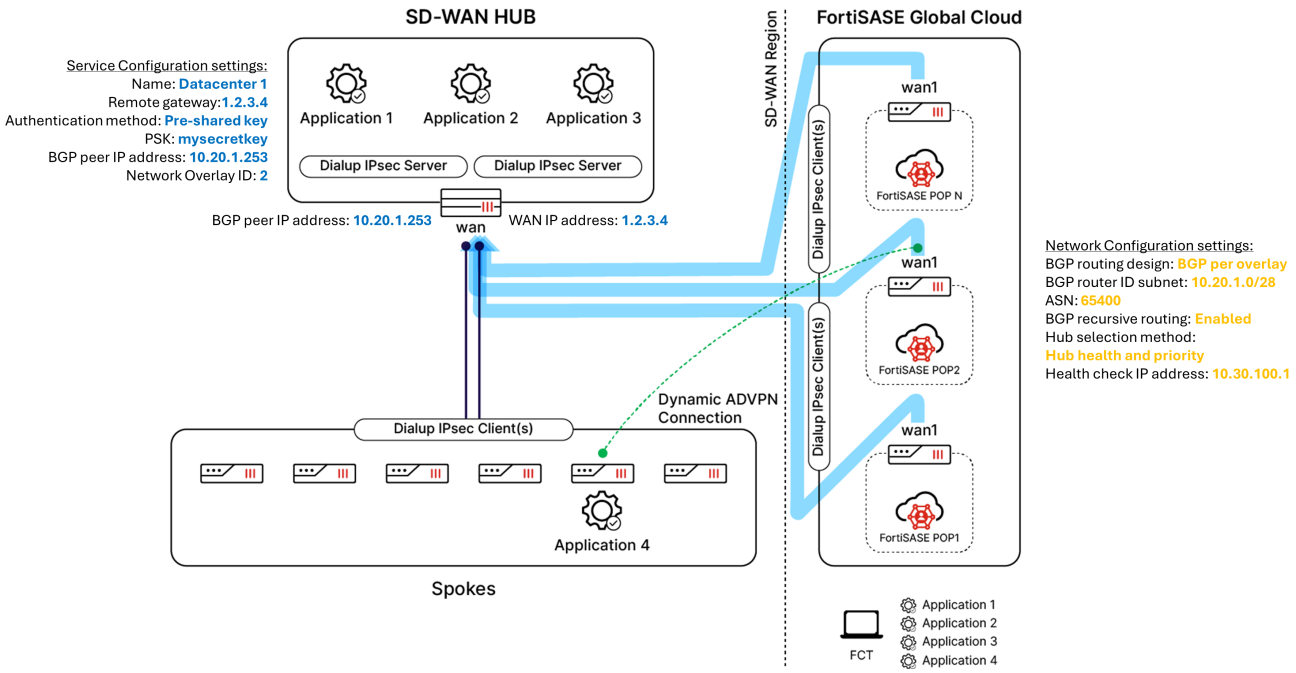
Secure private access

For securing FortiSASE remote user access to private TCP-based and UDP-based applications, FortiSASE supports secure private access (SPA) using SD-WAN or SPA using a next generation firewall converted to a standalone FortiSASE SPA hub. FortiSASE private access supports up to four FortiGate hubs.



For SPA use cases, the security points of presence (PoPs) act as spokes to the FortiGate hub (FortiGate SD-WAN hub or FortiSASE SPA hub), relying on IPsec VPN overlays and BGP to secure and route traffic between PoPs and the networks behind the organization's FortiGate hub.

FortiSASE security PoP and the organization’s FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN’s spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel.

The SPA use cases with FortiGate hubs allow traffic flow in the following directions:

From...	To...
Remote VPN users	FortiGate hubs (or spokes connected to hubs)
FortiGate hubs (or spokes connected to hubs)	Remote VPN users

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

The example network topology uses the following settings configured in FortiSASE:

Configuration setting	Value used in example network topology
Network Configuration settings	
BGP routing design	*BGP per overlay*
BGP router ID subnet	10.20.1.0/28
Autonomous system number (ASN)	65400
BGP recursive routing	Enabled
Hub selection method	*Hub health and priority*

Configuration setting	Value used in example network topology
Health check IP address	10.30.100.1
Service Connection settings	
Name	Datacenter 1
Remote gateway	1.2.3.4
Authentication method	*Pre-shared key*
Pre-shared key	mysecretkey
BGP peer IP address	10.20.1.253
Network Overlay ID	2

Prerequisites

For the FortiGate SD-WAN secure private access (SPA) use case, SD-WAN network deployments are expected to conform to Fortinet's best practices for SD-WAN architecture and deployment for the following topologies:

- SD-WAN with a single datacenter/hub
- SD-WAN with dual datacenters/hubs
- SD-WAN with up to four datacenters/hubs

For deployment details, see the 4-D FortiSASE SPA with a FortiGate SD-WAN Deployment Guide.

For the FortiGate next generation firewall (NGFW) SPA use case, you must first convert the NGFW to a standalone IPsec VPN hub. For deployment details, see the 4-D FortiGate NGFW to FortiSASE SPA Hub Conversion Deployment Guide (FortiOS 7.0.7+).

For the FortiGate NGFW SPA use case running FortiOS 7.2.4 and above, you can use the Fabric Overlay Orchestrator feature to convert the NGFW to a standalone IPsec VPN hub. For deployment details, see the 4-D FortiGate NGFW to FortiSASE SPA Hub Conversion using Fabric Overlay Orchestrator Deployment Guide (FortiOS 7.2.4+, 7.4.0+).

SPA license and account prerequisites

SPA requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection license and SPA FortiCloud account prerequisites.

Network restrictions

Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

The following protocols and ports are reserved for FortiSASE internal usage and you cannot use them for secure private access (SPA) connections. See Required services and ports on page 19:

- TCP port 8008
- TCP port 8010
- TCP port 8015
- TCP port 8020

If you must use these non-standard and reserved ports for SPA connections, open a FortiCare support ticket to request allowing these ports for SPA usage for your instance.

Configuring the FortiSASE security PoPs as the FortiGate hub's spokes

Before configuring secure private access (SPA) settings in the FortiSASE portal, to ensure proper SPA functionality, you must ensure that the FortiGate hub conforms to the deployment details (topologies and configuration settings) that the specific 4-D FortiSASE SPA deployment guide corresponding to your SPA use case covers as Prerequisites on page 89 mentions.

To allow FortiSASE remote users with SPA to resources behind your FortiGate hub (FortiSASE SPA hub/FortiGate SD-WAN hub) network, you can configure FortiSASE security points of presence (PoP) as spokes in your hub-and-spoke network in *Network* > *Secure Private Access*.

Configuration workflow

To configure SPA service connections (hubs), you must follow this configuration workflow in *Network* > *Secure Private Access*:

1. Click the *Network Configuration* tab at the top of the page and configure the common network configuration settings. See Configuring network configuration on page 91.
2. Click the *Service Connections* tab at the top of the page, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 94.

You cannot configure a service connection or hub without first configuring *Network Configuration* settings.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using BGP per overlay (default) or BGP on loopback. See the following table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay (default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke

Configuring network configuration

Before proceeding with configuring hubs or service connections, you must configure common secure private access (SPA) network configuration that all service connections use.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using BGP per overlay (default) or BGP on loopback. See the following table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay (default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke

You can use only a single BGP routing design method for all hubs and spokes. You cannot mix design methods.

Also, the BGP routing design method cannot be changed once saved. You must delete the service connection(s) and network configuration and reconfigure with a different BGP routing design method.

To configure SPA network configuration:

1. Go to *Network* > *Secure Private Access* and click the *Network Configuration* tab.
2. For the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select one of the following:
   - BGP per overlay (default selection)
   - BGP on loopback. FortiSASE automatically selects and grays out *BGP Recursive Routing* after you selecting this option.
3. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE validates the input and notifies you of any invalid values. See the following table:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • BGP per overlay (default)	BGP per overlay

Network attributes	Description	Example
	• BGP on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them.	
BGP router ID subnet	Available/unused subnet that can be used to assign loopback interface IP addresses used for BGP router IDs parameter on the FortiSASE security PoPs. /28 is the minimum subnet size. Typically, this BGP router ID subnet is a subnet within the overall BGP loopback summary range that is currently unused. For example, if the BGP loopback summary range is 10.20.1.0/24 then you can choose to configure 10.20.1.0/28 as the BGP router ID subnet if it is unused. For *BGP on loopback*, you must configure this subnet as a neighbor range in the hub BGP settings.	10.20.1.0/28
Autonomous system number (ASN)	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65400
BGP recursive routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails. For example, consider that this BGP configuration setting enabled and a FortiSASE security PoP's connectivity with hub 1 goes down. To ensure the security PoP can reach a network behind hub 1, it would route traffic to hub 2 first, then route it to hub 1 via its interhub connection, followed by routing the traffic to the desired destination network behind hub 1.	Enabled
Hub selection method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each PoP that meets lowest cost SLA requirements. A hub can be assigned a different priority level in different PoPs.	Hub health and priority

Network attributes	Description	Example
	• **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	
Health check IP address	IP address of a server behind the hub that should be used to set up the SD-WAN performance SLA rule.	10.30.100.1

Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

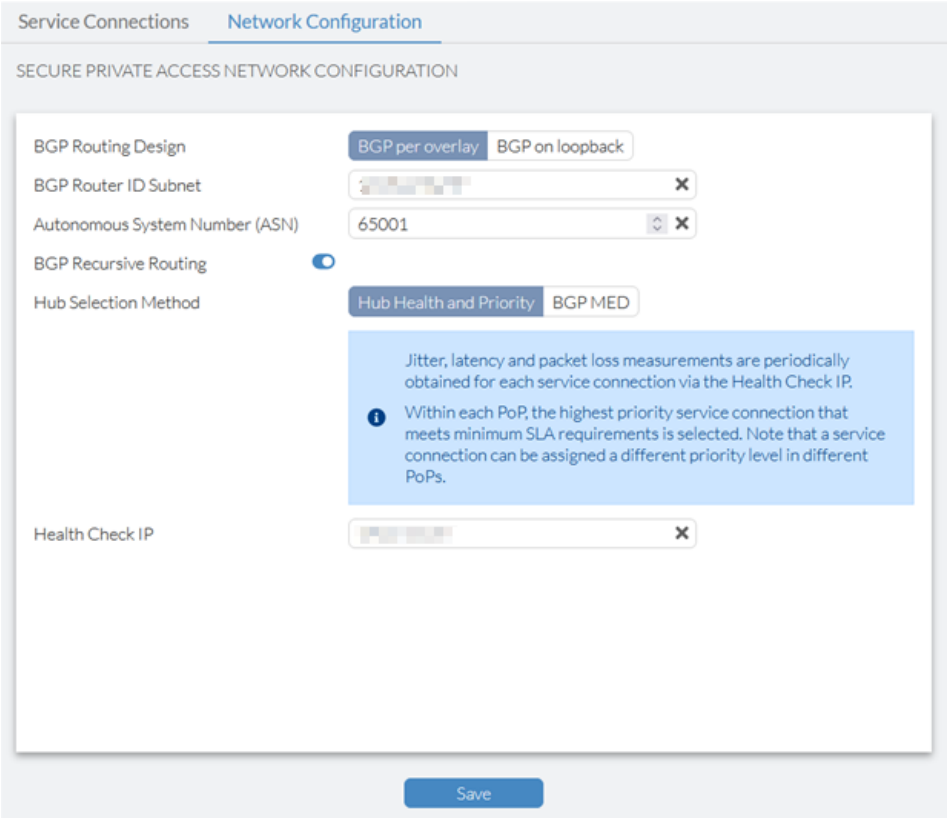
- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.

4. Click *Save*.



Configuring a new service connection

You can create a new service connection (hub) using one of the following BGP routing design methods:

- BGP per overlay (default)
- BGP on loopback

You configured the corresponding BGP routing design method in the *Network Configuration* tab.

After you create a service connection, you can update its authentication method using *Update Authentication Method*, namely, to switch from using a preshared key (PSK) to a certificate or vice-versa. You can also use this option to update the existing authentication method's settings, such as updating the PSK or updating the PKI user or certificate.

To configure service connections or hubs for BGP per overlay:

1. Go to *Network* > *Secure Private Access*.
2. On the *Service Connection* tab, click *Create*.
3. Fill in the rest of the fields with the attributes of the FortiGate hub or service connection. FortiSASE validates the input and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared key* (default) and *Certificate*.	Pre-shared key
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate that FortiSASE uses to validate the hub's certificate. You can directly create the PKI user from *+Create* or via *Configuration* > *PKI*, then select it here.	mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate for the FortiSASE security PoP to present. You must import this certificate into FortiSASE via *System* > *Certificates* as a *Local Certificate*.	Fortinet_Factory
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

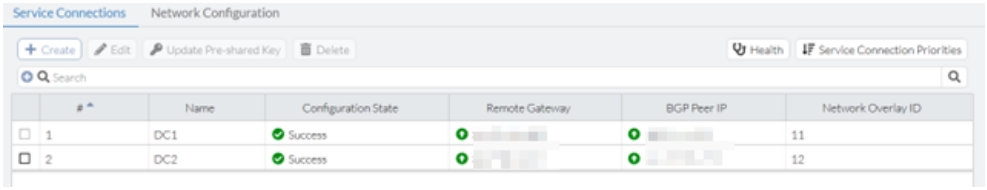
Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

4. Click *Save*.
5. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
6. (Optional) Repeat the steps to configure up to a total of four service connections as necessary to support your secure private access service connection network topology. The following shows the GUI after configuring two service connections:



For FortiSASE security points of presence (PoP), the SD-WAN performance SLA (health check) setting has the following parameters:

- **Latency threshold**: 120 ms
- **Jitter threshold**: 55 ms
- **Packet loss threshold**: 1%

Also, for FortiSASE security PoPs, the SD-WAN rule is configured with the lowest cost (SLA) mode, where the security PoPs choose the lowest cost link (highest priority hub) that satisfies the SLA to forward traffic.

In the SD-WAN rule used by each FortiSASE security PoP, the interface preference order matters when selecting links of equal cost (equal priority hubs). Therefore, to define interface preference order, you must configure service connections in FortiSASE in the desired order of preference from the most preferred hub to the least preferred hub.

To configure service connections or hubs for BGP on loopback:

1. Go to *Network* > *Secure Private Access*.
2. On the *Service Connection* tab, click *Create*.
3. For the *Create a New Secure Private Access Service Connection* step, fill in the fields with the attributes of the FortiGate hub or service connection. FortiSASE performs input validation and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1

Network attributes	Description	Example
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared key* (default) and *Certificate*.	Pre-shared key
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate that FortiSASE uses to validate the hub's certificate. You can directly create the PKI user from *+Create* or via *Configuration* > *PKI*, then select it here.	mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via *System* > *Certificates* as a *Local Certificate*.	Fortinet_Factory
ADVPN Route Tag	For *BGP on loopback* only, ADVPN route tag number for spoke to tag incoming routes advertised from a hub. See Enhanced BGP next hop updates and ADVPN shortcut override.	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

Because the following IP addresses ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.252.0.0/16
- 10.253.0.0/16
- 100.65.0.0/16

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

4. Click *Save*.
5. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
6. (Optional) Repeat the steps to configure up to a total of four service connections as necessary to support your secure private access service connection network topology.

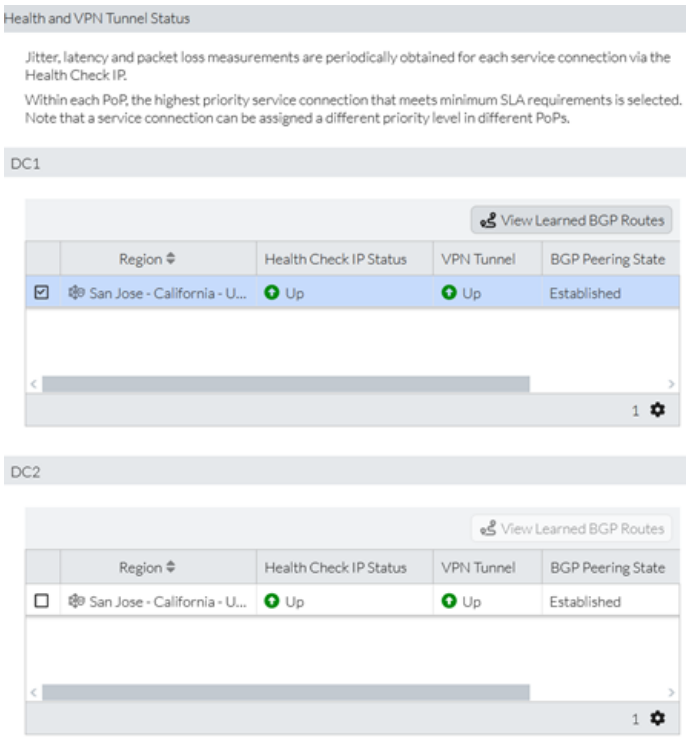
To update the authentication method settings for a service connection:

1. Go to *Network* > *Secure Private Access*.
2. On the *Service Connection* tab, click *Update Authentication Method*.
3. Select the *Authentication Method* and configure the corresponding parameter(s):
   a. *New Pre-shared Key* when *Pre-shared Key* is selected.
   b. *PKI User* and *Certificate* when *Certificate* is selected.
4. Click *OK*. Once FortiSASE successfully updates the authentication method for the service connection, it notifies you with the message *Authentication method updated successfully*.

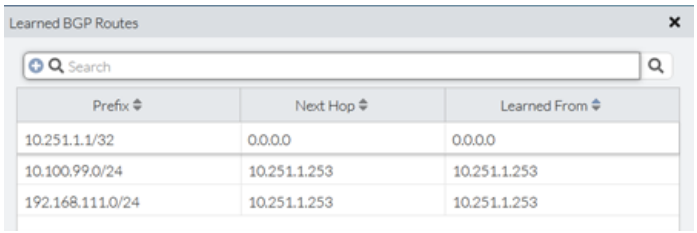
Viewing health and VPN tunnel status

Click the *Health* button at the top of the page to view the *Health and VPN Tunnel Status* page, which shows all configured hubs' health and VPN tunnel status. This page provides advanced monitoring of the IPsec VPN tunnel, BGP peering state, and health check IP status that you can use for troubleshooting advanced scenarios with configured hubs.

For example, you can view two hubs' health and VPN tunnel status from this page:



For any hub, selecting a point of presence and clicking *View Learned BGP Routes* displays the learned BGP routes for that hub. For example, the learned BGP routes for the example DC1 are as follows:

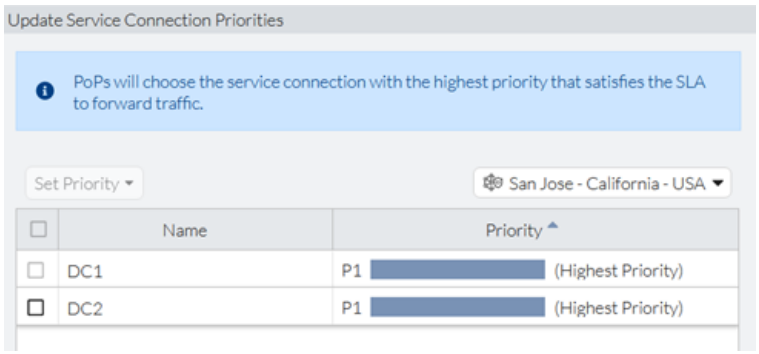


Updating service connection priorities

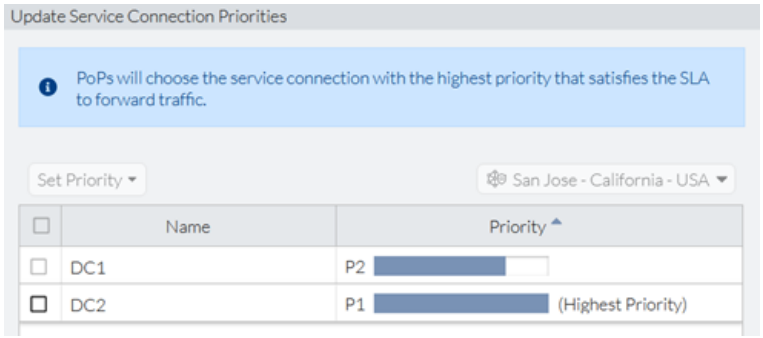
When you configure the hub selection method as hub health and priority within each point of presence (PoP), FortiSASE selects the highest priority hub that meets minimum SLA requirements. You can assign a hub a different priority level in different PoPs using the *Update Service Connection Priorities* page. A lower numerical cost value indicates a higher priority for a hub and vice-versa.

To update hub priorities:

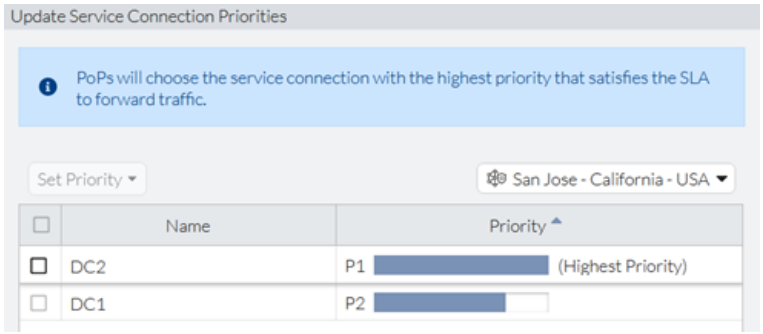
1. Go to *Network* > *Secure Private Access*. On the *Service Connections* tab, click *Update Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired PoP hub. The example selects the San Jose – California – USA security PoP.



3. Select the desired hub and do one of the following to set the priority:
   a. From the *Set Priority* dropdown list, select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
   b. Right-click the hub, select *Set Priority*, and select the desired priority. P1 is the highest priority, and P2 is the lowest priority.
4. Set the priority for each hub that will influence hub selection. The example modifies hub priorities so that DC1 has a priority of P2 and DC2 has a priority of P1:



5. Click *Apply* to save the updated priority values. The page sorts the hubs from highest to lowest priority:



6. (Optional) Repeat the steps to update hub priorities for other security PoPs.

Deleting a hub configuration

You cannot directly update hub configuration. You must delete any current configuration and reconfigure using new settings to update it.

To delete a hub configuration:

1. Go to *Network* > *Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

Configuring SPA using the Rest API

A FortiSASE administrator can perform secure private access (SPA) configuration using the FortiSASE REST API to manage the common SPA network connection and the SPA service connections to FortiGate SPA hubs and to retrieve the status of these connections. See Appendix C - REST API on page 328.

All SPA configuration operations are possible in the REST API except for viewing health and VPN tunnel status.

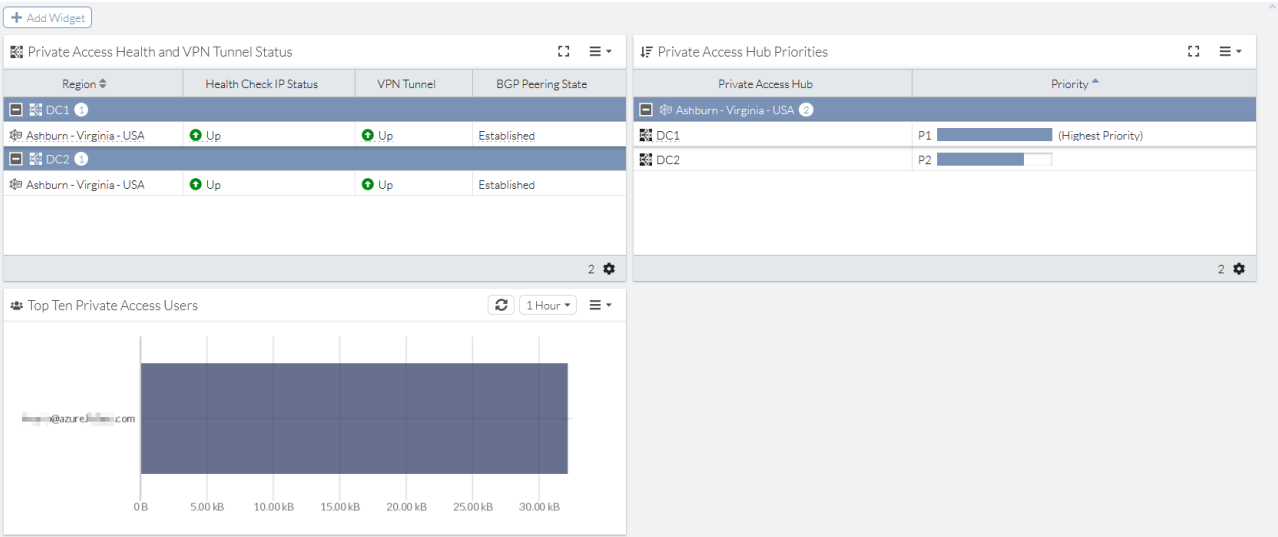
Only BGP on loopback supports multiple IPsec overlays in the REST API. Currently, this feature is only configurable using the REST API.

Monitoring private access hubs

To monitor private access hubs when you have configured them, view the following widgets in the *Dashboards* > *Private Access* page:

- Private Access Health and VPN Tunnel Status
- Private Access Hub Priorities
- Top Ten Private Access Users

The following provides private access widgets with data for two private access hubs:



Configuring a private access policy for remote VPN users and edge devices

To configure a private access policy from remote VPN users and edge devices to SPA hubs:

1. Go to *Configuration* > *Policies*.
2. Click the *Private Access* tab and then click the *To hubs* subtab.
3. Click *+Create* to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all FortiSASE VPN users and edge devices • *VPN Users*: remote endpoint users • *Edge Devices*: Edge devices such as FortiExtender • *Specify*: specify selected hosts and host groups if you selected *VPN Users* or authorized Edge devices if you selected *Edge Devices*.
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Service	Click + and select entries.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.

5. Click *OK*.

To configure a private access policy to remote users from SPA hubs:

The display of the *From hubs* subtab and resulting functionality requires a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification on page 24. Otherwise, the *From hubs* subtab does not display.

Currently, FortiSASE supports traffic from SPA hubs to remote VPN users only.

1. Go to *Configuration* > *Policies*.
2. Click the *Private Access* tab and then click the *From hubs* subtab.
3. Click *+Create* to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups.
Destination	• *All*: all FortiSASE users/devices • *VPN Users*: remote endpoint users
Service	Click + and select entries.
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.

5. Click *OK*.

To configure a FortiGate SPA hub firewall policy required for traffic from SPA hubs:

On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote VPN users via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote VPN users.

In this example, for the FortiGate SPA hub, the SPA overlay (IPsec VPN tunnel) is defined as *fgt_hub1* and the local connected networks DMZ_HQ and LAN_HQ are on port2 and port4, respectively. Therefore, we create a policy that allows traffic from the local connected networks on the hub to the FortiSASE remote VPN users.

1. On the FortiGate SPA hub, go to *Policy & Objects* > *Firewall Policy*.
2. Click *+Create New* to create a new policy.

3. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Incoming Interface	*DMZ_HQ (port2)* *LAN_HQ (port4)*
Outgoing Interface	*fgt_hub1*
Source	*all*
Destination	*All*
Schedule	*always*
Service	*ALL*
Action	*ACCEPT*
NAT	You can enable or disable NAT depending on the IP configuration of the organization's FortiGate SPA hub.
IP Pool Configuration	*Use Outgoing Interface Address*

4. Click *OK*.

Configuring a private access policy for SWG users

To configure a private access policy from SWG users to SPA hubs:

1. Go to *Configuration* > *SWG Policies*.
2. Click the *Private Access* tab and then click the *To hubs* subtab.
3. Click *+Create* to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• *All*: all HTTP and HTTPS traffic from SWG users • *Specify*: specify selected hosts and host groups
User	• *All Secure Web Gateway Users*: All SWG users • *Specify*: specify selected users or users groups
Destination	• *Private Access Traffic*: all private access traffic • *Specify*: specify selected private access hosts or host groups
Action	*Accept* or *Deny*
Profile Group	*Default* or *Specify* and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.

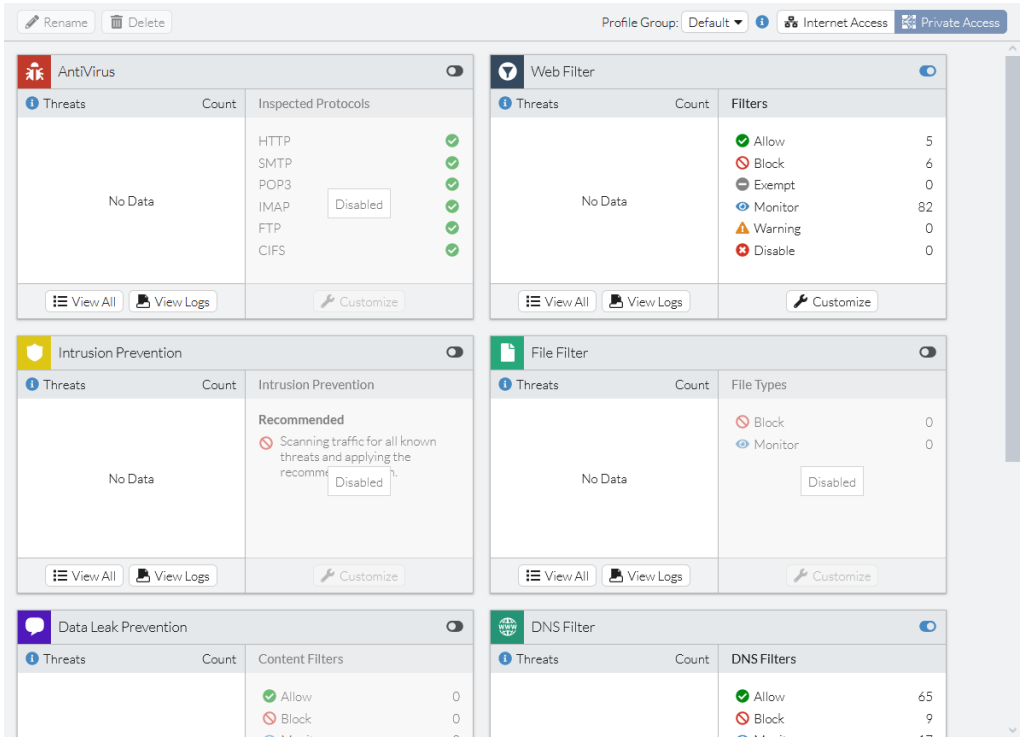
5. Click *OK*.

Configuring a private access security profile

To configure a private access security profile:

1. Go to *Configuration* > *Traffic* > *Security*.
2. In the top right corner, click *Secure Private Access*.

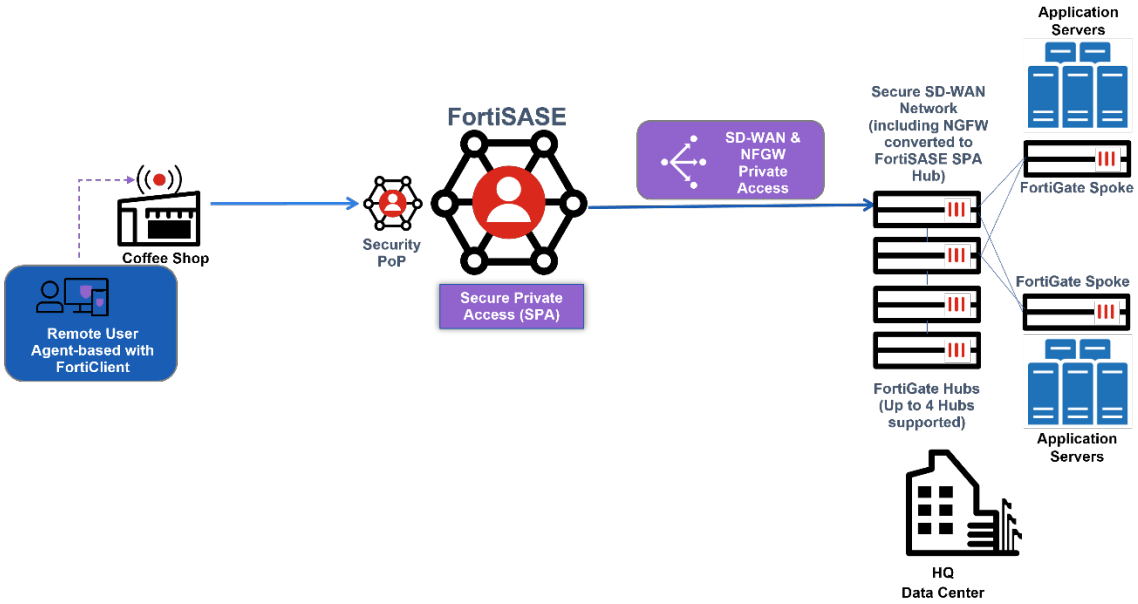
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



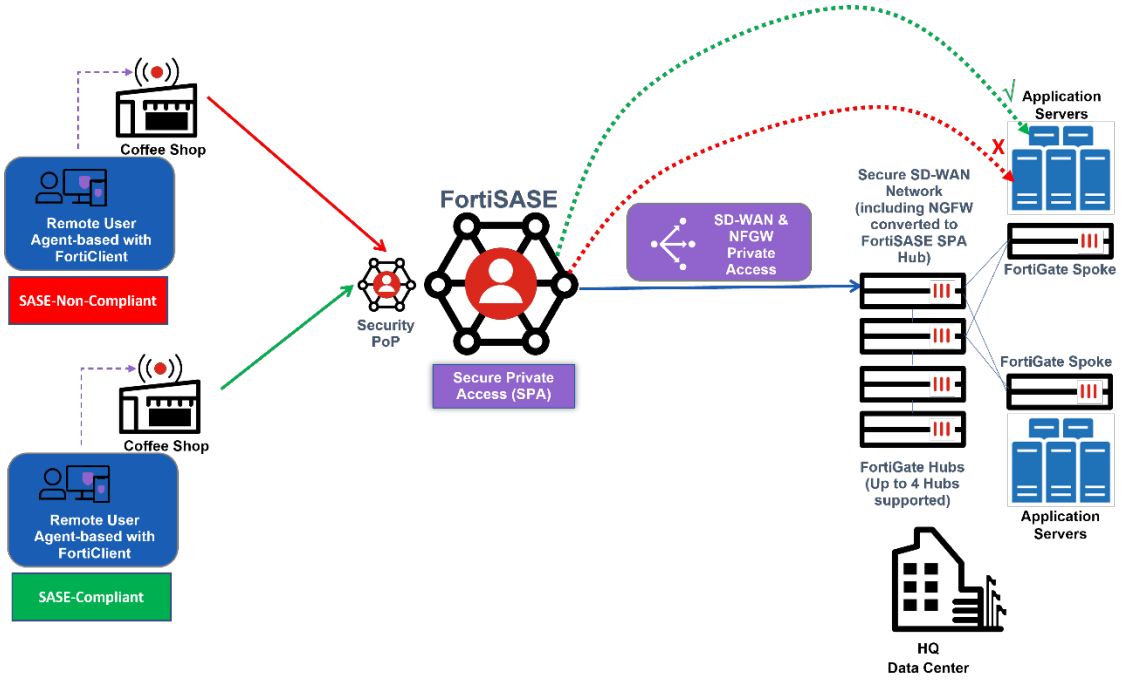
The security settings for internet and private access are identical. For details on configuring security settings, see Security on page 145.

Configuring ZTNA tags in private access policies

By default, for the secure private access (SPA) use cases using a FortiGate hub configured through the *Secure Private Access* page, all FortiSASE agent-based remote users have unrestricted access to private applications behind the hub network through an Allow-All Private Traffic private access policy.



To restrict SPA to private applications of any protocol (TCP, UDP, ICMP, and so on) behind a FortiGate hub, in the FortiSASE portal you can configure zero trust network access (ZTNA) tagging rules that apply ZTNA tags to remote users based on specified endpoint posture checks. You can then specify these tags as the source in a dynamic private access policy to deny or allow access as desired.



Using ZTNA tags to configure dynamic policies

You can use tags to build dynamic policies that you do not need to manually reconfigure whenever an endpoint's status changes. For example, consider that you want to deny Windows endpoints without antivirus (AV) installed and running

as detected by FortiClient from accessing private applications behind the FortiGate hub. You would configure the following:

- Rule that applies a SASE-Compliant tag to Windows endpoints that FortiClient detects as having AV software installed and running
- Rule that applies a SASE-Non-Compliant tag to Windows endpoints that FortiClient detects as not having AV software installed
- Private access policy that allows Windows endpoints with the SASE-Compliant tag to access a specific server behind the FortiGate hub
- Private access policy that denies Windows endpoints with the SASE-Non-Compliant tag from accessing a specific server behind the FortiGate hub

As FortiSASE receives information from endpoints, it dynamically removes and applies the SASE-Non-Compliant tag to endpoints. For example, if an endpoint that previously had the SASE-Non-Compliant tag applied has its AV software installed or enabled as detected by FortiClient, then FortiSASE automatically removes the SASE-Non-Compliant tag from the endpoint and applies the SASE-Compliant tag instead. Consequently, the endpoint would then be able to access private applications behind the FortiGate hub.

Therefore, a dynamic policy is a policy that has one or more zero trust network access tags specified as its source.

For details on configuring dynamic tags and policies, see Tagging on page 257.

Configuration workflow

You can follow this configuration workflow, which the document describes in detail using the example configuration of a dynamic private access policy that allows access to private applications, which in this example is a private server behind the FortiGate hub:

1. Configure a zero trust network access (ZTNA) tagging rule set for compliant endpoints.
2. Configure a ZTNA tagging rule set for non-compliant endpoints.
3. Configure a dynamic private access policy to allow access to a specific private server from compliant endpoints.
4. Configure a dynamic private access policy to deny access to a specific private server from non-compliant endpoints.
5. Test the dynamic private access policies using ICMP ping to the specific private server from a compliant endpoint and from a non-compliant endpoint, respectively.

A similar workflow applies to a private access policy that allows or denies access to applications of any other protocols besides ICMP, such as TCP or UDP applications.

Configuring ZTNA rule sets to dynamically tag agent-based remote users

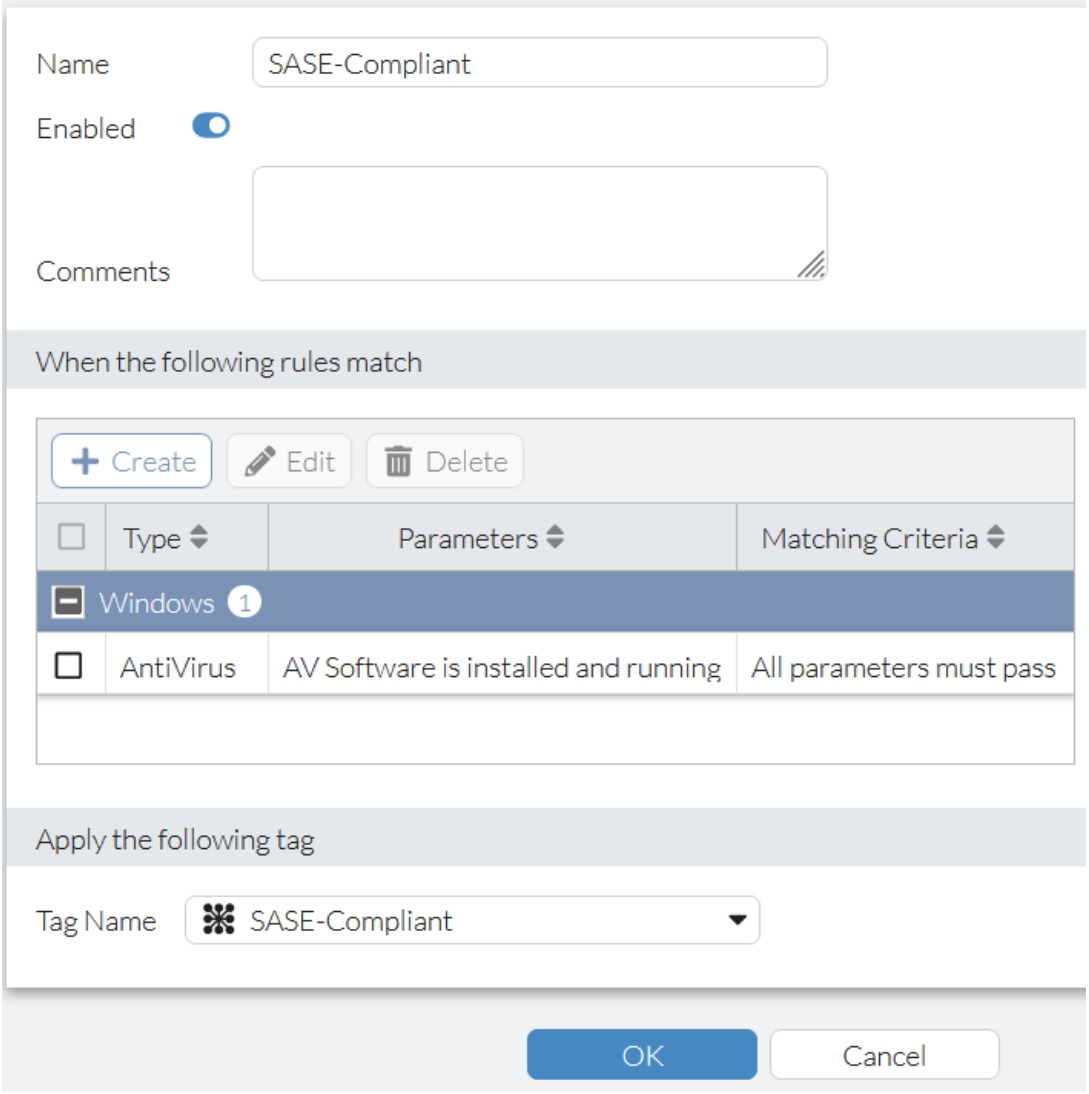
This example demonstrates how to configure zero trust network access (ZTNA) tag names and ZTNA tagging rule sets with the following posture checks:

- Endpoint is running Windows and has antivirus (AV) software installed and running
- Endpoint is running Windows and does not have AV software installed or running

To configure a ZTNA tagging rule set for compliant endpoints:

1. Go to *Configuration* > *ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.

4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.
6. Configure the Severity Level rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.



To configure a ZTNA tagging rule set for non-compliant endpoints:

1. Go to *Configuration* > *ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.

5. Under *When the following rules match*, click *Create*.
6. Configure the Severity Level rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. Select *Negate*.
   d. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.

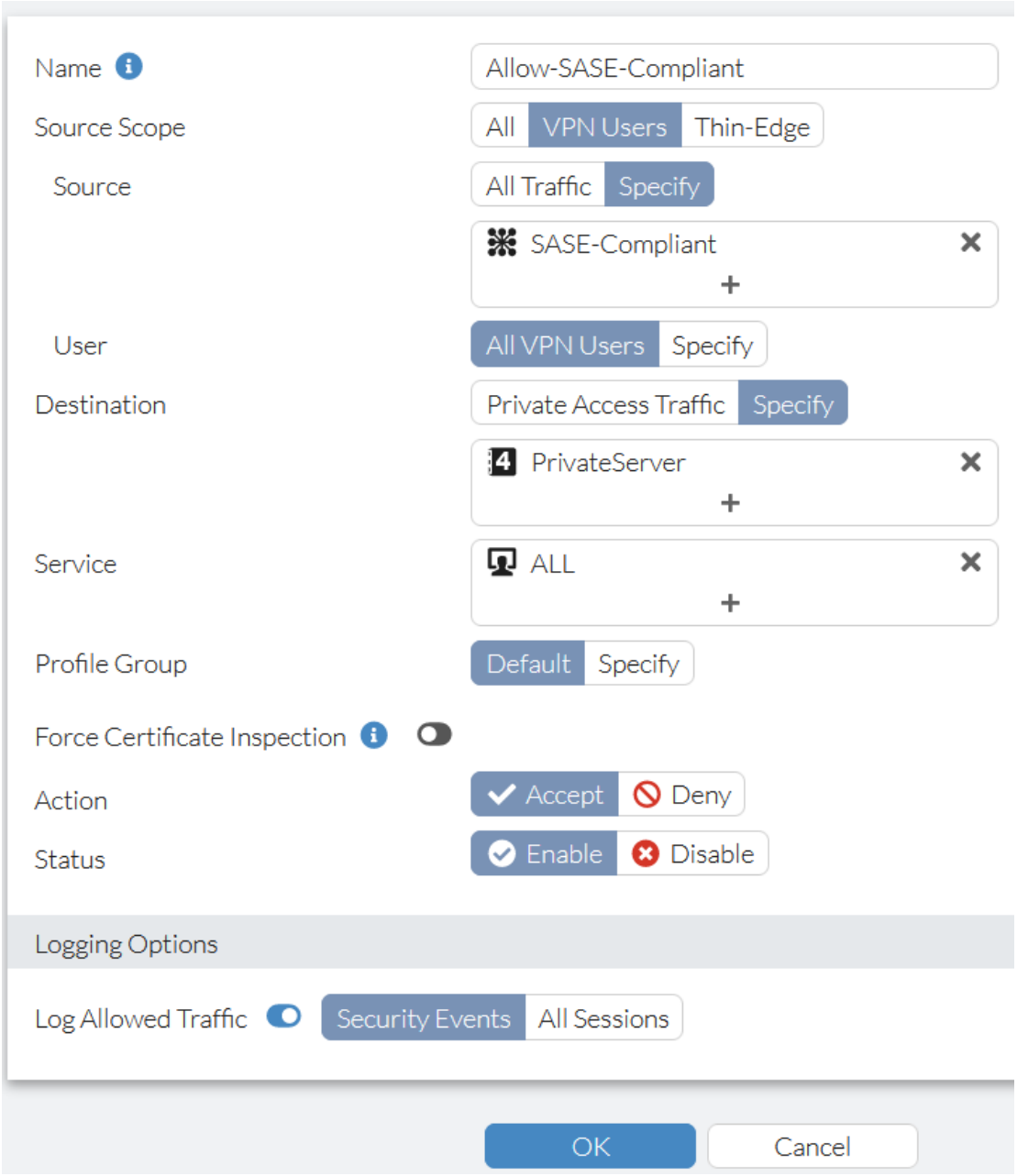
Configuring dynamic private access policies using ZTNA tags

This example demonstrates how to configure dynamic private access policies using the zero trust network access tags that you created in Configuring ZTNA rule sets to dynamically tag agent-based remote users on page 108 to allow endpoints tagged as SASE-Compliant with access to selected private resources and to deny access to selected private resources for endpoints tagged as SASE-Non-Compliant.

To configure a dynamic private access policy for compliant endpoints:

1. Go to *Configuration* > *Policies*.
2. Select *Secure Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *VPN Users*.
   c. In the *Source* field, select *Specify* and click +. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Compliant* tag.
   d. For *Destination*, select *Specify*, click +, and in the *Select Entries* panel click +*Create* and click *IPv4 Host* to a create a new host for the specific server as follows:
      i. For *Location*, select *Private Access Hub*.
      ii. For *Category*, *IPv4 Host* is selected.
      iii. In the *Name* field, enter the desired name. In this example, the name is PrivateServer.
      iv. From the *Type* dropdown list, select *Subnet*.
      v. In the *IP/Netmask* field, enter 10.100.99.101/32.
      vi. Click *OK*.
      Select the newly created host to set it as the *Destination*.
   e. For *Service*, click + and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Accept*.
   g. For *Status*, select *Enable*.

5. Click *OK*.

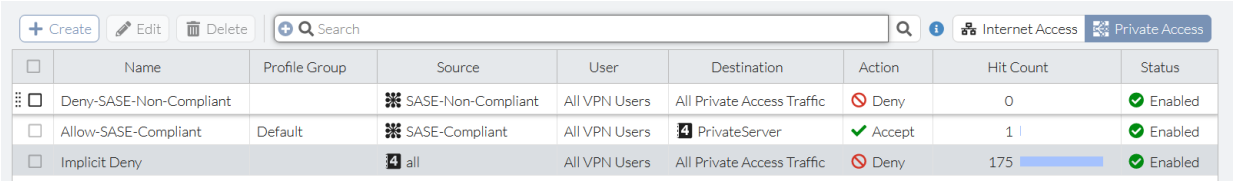


6. In *Configuration* > *Policies* with *Secure Private Access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.

To configure a dynamic private access policy for non-compliant endpoints:

1. Go to *Configuration* > *Policies*.
2. Select *Secure Private Access* to display the list of private access policies
3. Click *Create*.

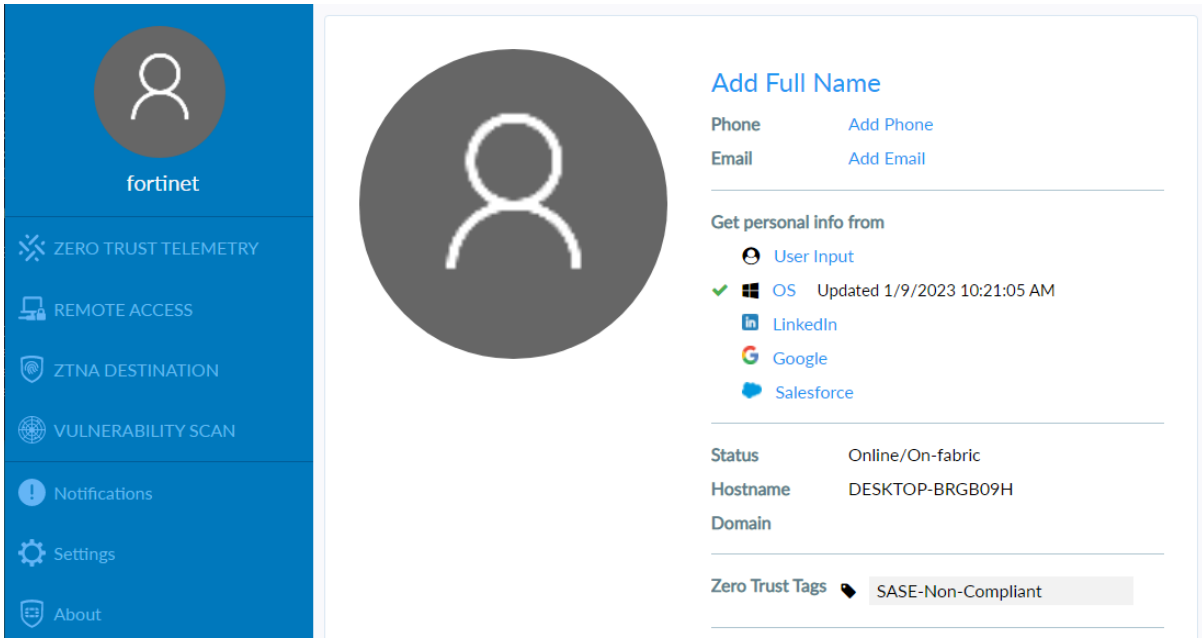
4. Configure the policy:
   a. For *Name*, enter Deny-SASE-Non-Compliant.
   b. For *Source Scope*, select *VPN Users*.
   c. In the *Source* field, select *Specify* and click +. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Non-Compliant* tag.
   d. For *Destination*, select *Private Access Traffic*.
   e. For *Service*, click + and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Deny*.
   g. For *Status*, select *Enable*.
5. Click *OK*.
6. In *Configuration* > *Policies* with *Secure Private Access* selected, do the following:
   a. Ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.
   b. Delete the Allow-All Private Traffic and Allow-All Private Traffic Thin-edge policies.



Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *Configuration* > *Endpoints* > *Profiles*.
2. Enable *Show tags on FortiClient*.
3. Click *Apply*. When this option is enabled, detected tags appear on the FortiClient avatar page.



To test that FortiSASE allows a FortiClient endpoint tagged as SASE-Compliant access to a private server:

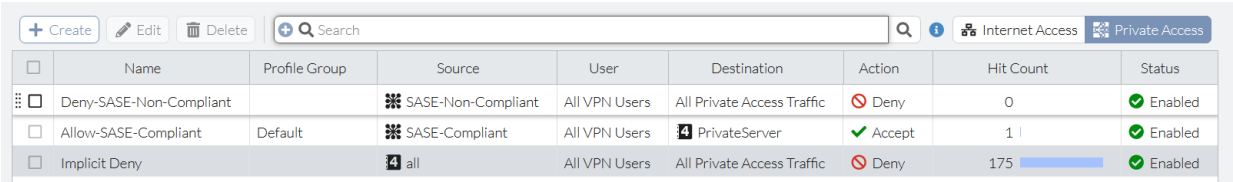
1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *On* as Stay protected with Windows Security describes. This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ping succeeded since FortiSASE allows access:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=136ms TTL=62

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 137ms, Average = 136ms
```

8. In FortiSASE, in *Configuration* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count increased and that the Deny-SASE-Non-Compliant dynamic private access policy hit count has not changed.



To test that FortiSASE denies a FortiClient endpoint tagged as SASE-Non-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *Off* as Stay protected with Windows Security describes. This turns off AV and ensures that FortiSASE dynamically tags the endpoint as non-compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ICMP ping has timed out since access to the specific server is denied:

```
C:\> ping 10.100.99.101
```

```
Pinging 10.100.99.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

8. In FortiSASE, in *Configuration* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count has not changed and that the Deny-SASE-Non-Compliant dynamic private access policy hit count increased.

Verifying IPsec VPN tunnels on the FortiGate hub

Verify that the IPsec VPN tunnels immediately appear on the FortiGate hub from all configured FortiSASE security points of presence(PoP).

On the FortiGate hub, verify that the IPsec VPN tunnels from the FortiSASE PoPs acting as spokes by going to *Dashboard* > *Network* and clicking the *IPsec* widget to expand it.

To verify IPsec VPN tunnels using the CLI:

1. Run at least one of the following commands. For a VDOM-enabled hub FortiGate, enter the proper VDOM before running the command(s):
```
diagnose vpn ike gateway list
diagnose vpn tunnel list
get vpn ipsec tunnel summary
```
   a. For `diagnose vpn ike gateway list`, confirm that the phase 1 IKE security associations (SA) for the FortiSASE security PoPs with corresponding peer IDs are established. Confirm that the IKE SA and IPsec VPN SA show created and established as 1/1. The following shows sample output for this command:

```
vd: root/0
name: ToSpokes_1
version: 2
…
created: 923s ago
peer-id: region8-fos001-tiui7pzu-1
…
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  …
  direction: responder
  status: established 923-923s ago = 10ms
  proposal: aes128-sha256
  child: no
  …
  PPK: no
  message-id sent/recv: 1/2
  lifetime/rekey: 86400/85206
  DPD sent/recv: 00000001/00000001
```

```
    peer-id: region8-fos001-tiui7pzu-1
```

2. For `diagnose vpn tunnel list`, confirm that the phase 2 IPsec VPN SAs for the FortiSASE security PoPs are established. Confirm that the SA field exist and are populated. The following shows sample output for this command:

```
name=ToSpokes_1 ver=2 serial=3ba 208.85.68.228:4500->154.52.6.89:52270 tun_
id=10.150.160.2 tun_id6=::10.0.3.147 dst_mtu=1500 dpd-link=on
 weight=1
bound_if=25 lgwy=static/1 tun=intf/2 mode=dial_inst/3 encap=none/9096 options
[2388]=npu rgwy-chg rport-chg frag-rfc  run_state=0 accept_
traffic=1 overlay_id=0
parent=ToSpokes index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0 ad=s/1
stat: rxp=2689 txp=1042 rxb=16418 txb=18338
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=52270
proxyid=ToSpokes proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42258/0B replaywin=2048
       seqno=411 esn=0 replaywin_lastseq=00000a80 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=fd64b472 esp=aes key=16 0ab999cd40bc420cc78556f84b37747f
       ah=sha1 key=20 2e9f19e91d696d530adefb3d219ad1c74d08dcd8
  enc: spi=14c9a05c esp=aes key=16 5446e233d666319b8f88fd1768f774b0
       ah=sha1 key=20 15989dc3ef5fd1d0b385df93241e0d6a0b373826
  dec:pkts/bytes=2689/16346, enc:pkts/bytes=1042/21844
  npu_flag=03 npu_rgwy=154.52.6.89 npu_lgwy=208.85.68.228 npu_selid=33d dec_npuid=1
enc_npuid=1
```

3. For `get vpn ipsec tunnel summary`, confirm that the phase 2 IPsec VPN selectors for the FortiSASE security PoPs are sending and receiving traffic. Confirm that `selectors(total,up): 1/1`, `rx(pkt,err)`, and `tx(pkt,err)` are non-zero. The following shows sample output for this command:

```
'ToSpokes_0' 154.52.29.50:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx
(pkt,err): 1043/0
'ToSpokes_1' 154.52.6.89:52270  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx
(pkt,err): 1042/0
'ToSpokes_2' 50.208.126.11:0  selectors(total,up): 1/1  rx(pkt,err): 22149/0  tx
(pkt,err): 55050/37
…
'ToSpokes_4' 206.47.184.245:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0
tx(pkt,err): 1043/0
…
```

Testing private access connectivity to FortiGate hub network from remote VPN users and edge devices

By using ping, you can verify access to the FortiGate hub network from FortiSASE remote users, namely, FortiClient users connected to FortiSASE in FortiClient agent-based mode and users behind FortiSASE edge devices.

For example, from a FortiClient user connected to FortiSASE, use ping within a Windows Command Prompt to verify access to a host behind the FortiGate hub internal network. The example pings 10.50.101.50, which is on an internal network. The following shows sample output:

```
C:\>ping 10.50.101.50
Pinging 10.50.101.50 with 32 bytes of data:
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=80ms TTL=62
Reply from 10.50.101.50: bytes=32 time=84ms TTL=62
```

Testing private access connectivity to FortiGate hub network from remote SWG users

This example requires *System* > *SWG Configuration* and *Configuration* > *SWG User SSO* to be configured appropriately. See SWG client onboarding on page 286 and Configuring FortiSASE with Entra ID SSO in SWG agentless mode on page 218.

By default, all SWG users can access all private access resources. You can limit SWG user access to private access resources by creating a private access policy for SWG users. See Configuring a private access policy for SWG users.

You can verify access to the FortiGate hub network from FortiSASE SWG users by using a web browser to access a host on the hub local network.

For example, consider the case when a host on the hub local network has an HTTP server running on 10.100.99.101 and only the default private access policy for SWG users is in place in FortiSASE.

To test private access connectivity to FortiGate hub network from remote SWG users:

1. From a web browser configured for SWG enter http://10.100.99.101.
2. If this is the first time going out to the internet, you will be prompted by SAML SSO to enter your credentials.
3. After entering your credentials, you should be able to access the web site at http://10.100.99.101 .

Testing private access connectivity from FortiGate hub network to remote VPN users

This test depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification on page 24.

You can verify access from the FortiGate hub network to FortiSASE VPN users, namely FortiClient users connected to FortiSASE in FortiClient agent-based mode using ping.

From a host behind the FortiGate hub internal network, use ping to verify access to a FortiClient user connected to FortiSASE

The example pings the FortiClient user with 100.65.0.1 from 10.100.99.104, which is a host on an internal network. The following shows sample output:

```
root@internal-server-01:~# ping 100.65.0.1
PING 100.65.0.1 (100.65.0.1) 56(84) bytes of data.
64 bytes from 100.65.0.1: icmp_seq=1 ttl=126 time=73.3 ms
64 bytes from 100.65.0.1: icmp_seq=2 ttl=126 time=72.5 ms
64 bytes from 100.65.0.1: icmp_seq=3 ttl=126 time=74.0 ms
64 bytes from 100.65.0.1: icmp_seq=4 ttl=126 time=72.1 ms
^C
--- 100.65.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 72.127/73.008/74.034/0.735 ms
```

Verifying BGP routing on the FortiGate hub

To verify that all BGP peering is up on the FortiGate hub:

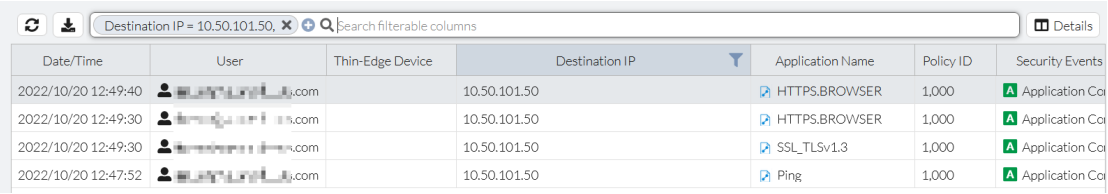
1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:
   ```
   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes
   ```
2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Static & Dynamic Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Verifying private access traffic in FortiSASE portal

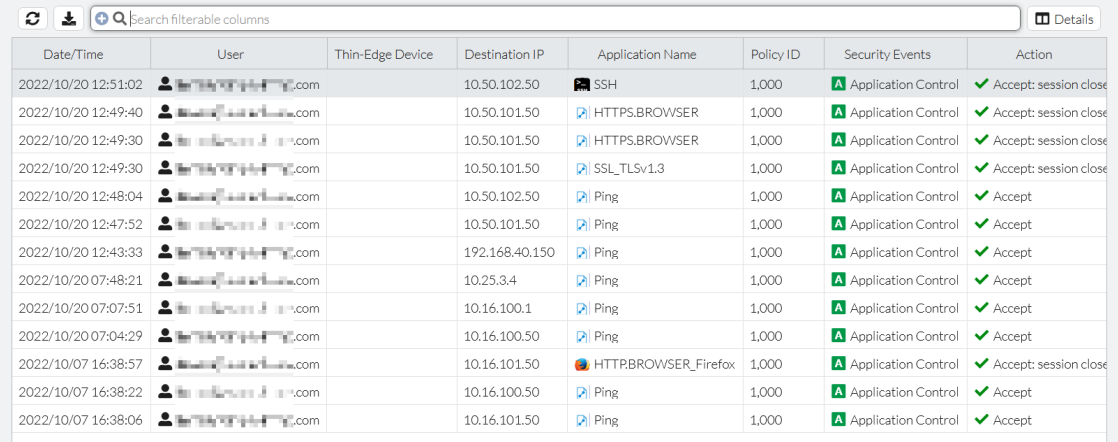
In the FortiSASE portal, you can verify traffic from FortiSASE remote users has reached private access destinations through these methods:

- From *Analytics* > *Logs* > *Traffic* by viewing either the *All Internet and Private Access Traffic* page or the *Private Access Traffic* page
- From *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* and filtering on the private access destination IP address

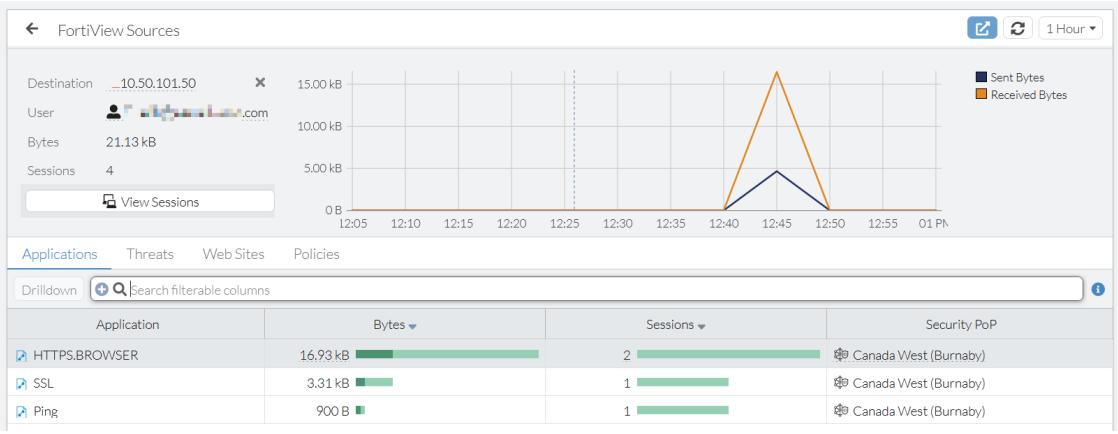
Following is an example of the *Analytics* > *Logs* > *Traffic* > *All Internet and Private Access Traffic* page, filtered for the private access destination IP address 10.50.101.50.

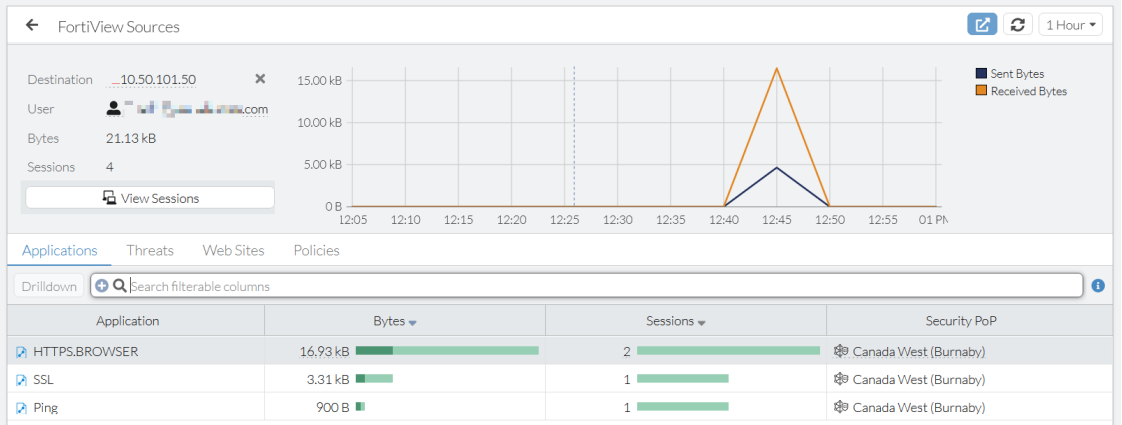


Following is an example of the *Analytics* > *Logs* > *Traffic* > *Private Access Traffic (To Hubs)* page.



Following are examples of the *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* pages, filtered on the private access destination IP address 10.50.101.50.





Verifying private access traffic from hubs

Verifying private access traffic from SPA hubs to FortiSASE remote users depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification on page 24.

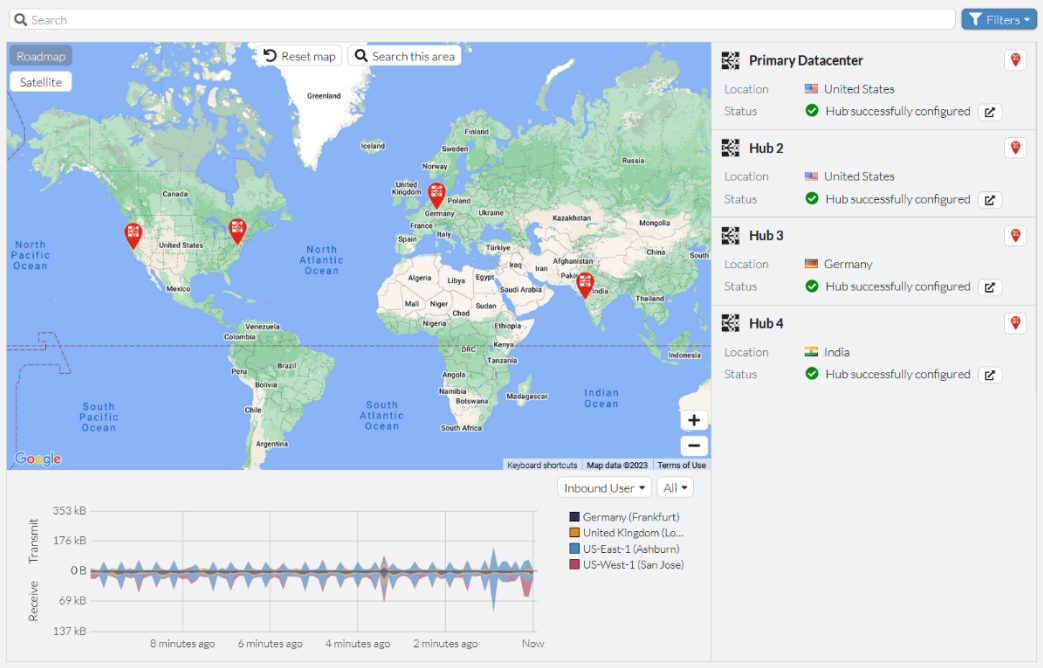
In the FortiSASE portal, you can verify traffic from SPA hub sources (local networks or connected spokes) has reached FortiSASE remote user destinations through these methods:

- From *Analytics* > *Logs* > *Traffic* by viewing *All Internet and Private Access Traffic* or *Private Access Traffic (From Hubs)*
- From *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* and filtering on the remote VPN user destination IP address

Verifying private access hub status and location using the asset map

The *Network* > *Asset Map* page in the FortiSASE portal supports filtering on *Private Access Hub* assets to display their status and geographical location.

Following is an example of the asset map filtered on *Private Access Hub* assets.



Managed Endpoints

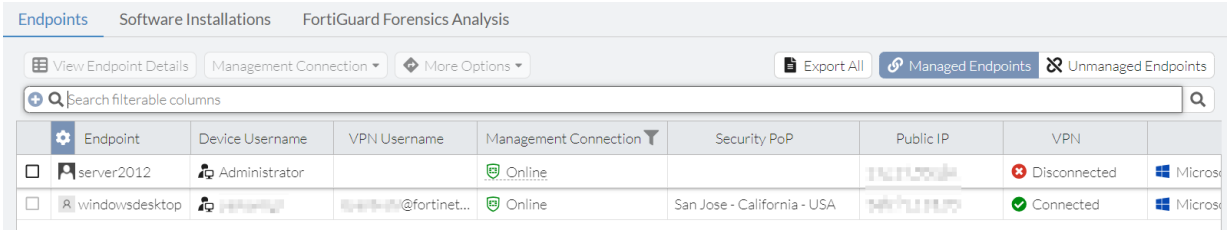
You can view managed endpoints via the *Network* > *Managed Endpoints* page.

Alternatively, you can display the Managed Endpoints status widget or status monitor under Dashboards as follows:

- Go to *Dashboards* > *Status* and under the *Managed Endpoints* widget, click *Click to Expand*. If this widget does not exist, add a new Managed Endpoints widget as Adding a custom dashboard on page 26 describes.
- Go to an existing Managed Endpoints monitor. If this monitor does not exist, add a new Managed Endpoints monitor as Adding a custom monitor on page 28 describes.

The page, status widget, and status monitor all display a list of endpoints that show endpoint information, including but not limited to the following:

- Device username
- VPN username
- Management connection status
- Security point of presence
- Public IP address
- VPN status
- Platform
- Vulnerabilities detected
- FortiClient version and ID
- Zero trust network access tags



The *Managed Endpoints* view contains the following buttons at the top of the page:

- When an endpoint is selected, you can use the *View Endpoint Details* button to display detailed endpoint information that FortiClient gathers on the endpoint device.
- The *Management Connection* button allows enabling/disabling the management connection for endpoints.
- When the endpoint has a *Connected* VPN status, you can click *More Options* to access the following actions:
  - *Export Diagnostic Logs*. You can only export diagnostic logs for online Windows endpoints.
  - *View VPN Session*
  - *Show in FortiView*
  - *Show Matching Traffic Logs*
- The *Export All* button exports the list of endpoints in a CSV file format that includes endpoint details such as device username name, IP and MAC addresses, FortiClient version, and so on.

  You can toggle between *Managed Endpoints* and *Unmanaged Endpoints* views.

Management Connection button

By default, the management connection for all endpoints is enabled. Therefore, you do not need to enable the management connection for an endpoint when you have not yet disabled it.

You can remove an endpoint from management by disabling its management connection with the following results:

- The endpoint is permanently excluded from management and cannot register with FortiSASE using an invitation code unless its management connection is reenabled.
- FortiSASE removes the endpoint profile and zero trust network access (ZTNA) tagging settings from the selected endpoint.
- A license seat is freed up for use by other endpoints.

After an endpoint has previously been removed from management, you can add it to management by enabling its management connection with the following results:

- FortiSASE is now managing the endpoint and the endpoint is allowed to register with FortiSASE using an invitation code.
- FortiSASE applies the endpoint profile and ZTNA tagging settings configured in *Configuration* > *Profiles* and *Configuration* > *ZTNA Tagging* respectively to the selected endpoint.
- The endpoint uses up a license seat.

To remove an endpoint from management:

1. Go to the *Managed Endpoints* page, status widget, or status monitor.
2. Click *Managed Endpoint* to enter that view.
3. Select the desired endpoint.

4. Click *Management Connection* > *Disable*. After disabling the endpoint's management connection, the endpoint should disappear from the *Managed Endpoints* view and appear in the *Unmanaged Endpoints* view.

When you remove an endpoint from management by disabling its management connection, in FortiClient the endpoint's zero trust telemetry connection and Remote Access FortiSASE VPN connection will both be disconnected.

The *Disable* option within *Management Connection* is not equivalent to the *Deregister* button in previous FortiSASE versions.

In previous versions, *Deregister* just disconnected the endpoint from FortiSASE and allowed the possibility for the endpoint to remain managed and reregister with FortiSASE.

Currently, once you configure *Management Connection* > *Disable* for an endpoint, it is permanently excluded from management. Namely, it is considered an unmanaged endpoint, and cannot register with FortiSASE.

To allow an unmanaged endpoint to be managed by and register with FortiSASE, you must select the endpoint and configure *Management Connection* > *Enable*.

To add an endpoint to management when it has been previously removed from management:

1. Go to the *Managed Endpoints* page, status widget, or status monitor.
2. Click *Unmanaged Endpoint* to enter that view.
3. Select the desired endpoint.
4. Click *Management Connection* > *Enable*. After enabling the endpoint's management connection, the endpoint disappears from the *Unmanaged Endpoints* view and does not appear in the *Managed Endpoints* view until it reconnects to FortiSASE.

Examples

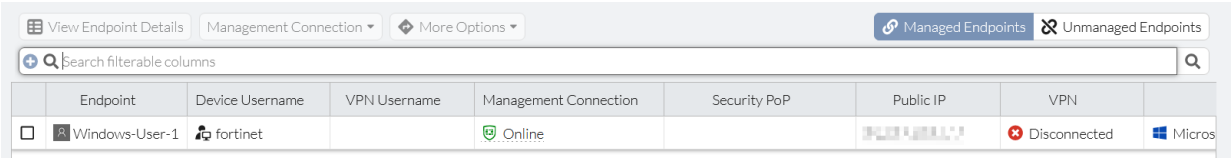
The following topics provide examples of actions you can perform from *Managed Endpoints*.

Example: Confirming an endpoint is added to management by default

To confirm an endpoint is added to management by default:

1. Initially, the desired endpoint has not yet attempted to connect to FortiSASE. Go to *Network* > *Managed Endpoints*, click the *Unmanaged Endpoints* view and confirm the endpoint is not yet visible there.
2. Go to *Configuration* > *Users* and click *Onboard Users*.
3. Set *FortiClient Installer* to *Download*.
4. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
5. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint successfully establishes a zero trust telemetry connection with FortiSASE. Upon connection, FortiClient receives an endpoint policy from FortiSASE. A system tray bubble message displays once the download completes.
6. Go to *Network* > *Managed Endpoints* and click *Managed Endpoints*. Confirm the endpoint is visible in that view and that the *Management Connection* is *Online*. If the endpoint reboots, it continues to establish its zero trust telemetry

connection with FortiSASE and receives an endpoint policy each time.



Example: Removing an endpoint from management

The *Disable* option within *Management Connection* is not equivalent to the *Deregister* button in previous FortiSASE versions.

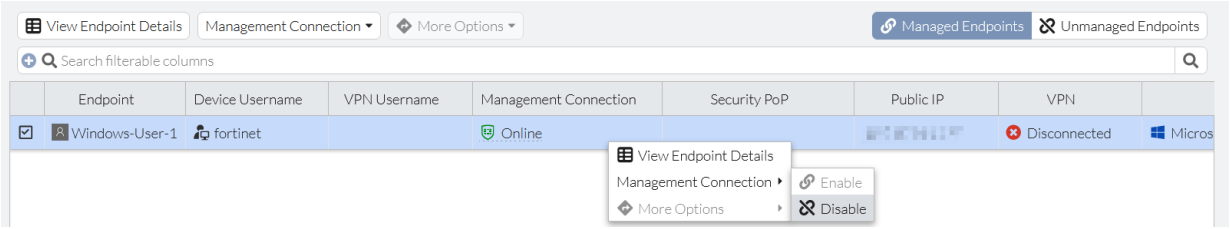
In previous versions, *Deregister* just disconnected the endpoint from FortiSASE and allowed the possibility for the endpoint to remain managed and reregister with FortiSASE.

Currently, once you configure *Management Connection* > *Disable* for an endpoint, it is permanently excluded from management. Namely, it is considered an unmanaged endpoint, and cannot register with FortiSASE.

To allow an unmanaged endpoint to be managed by and register with FortiSASE, you must select the endpoint and configure *Management Connection* > *Enable*.

To remove an endpoint from management:

1. Consider that the device has been managed and is registered to and connected to FortiSASE. Go to *Network* > *Managed Endpoints*, click the *Managed Endpoints* view, and confirm the endpoint is visible there.
2. Select the endpoint, select *Management Connection* > *Disable*, and click *OK* to confirm. In FortiClient after the telemetry sync timer elapses, the endpoint's zero trust telemetry connection and the FortiSASE VPN connection both disconnect after previously having been connected.

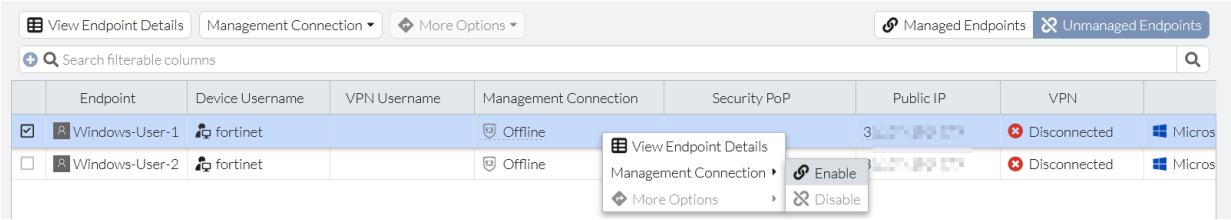


3. Confirm that the endpoint has disappeared from the *Managed Endpoints* view.
4. Go to *Network* > *Managed Endpoints* and click *Unmanaged Endpoints*. Confirm the endpoint is visible in that view.
5. Go to *Configuration* > *Users* and click *Onboard Users*.
6. Set *FortiClient Installer* to *Download*.
7. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
8. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint no longer successfully establishes its zero trust telemetry connection with FortiSASE since you have excluded it from management.
9. If the endpoint reboots, repeat step 8. FortiClient attempts to connect to FortiSASE and never succeeds with registering and receiving an endpoint policy each time. This confirms that the unmanaged endpoint has been excluded from management as desired.

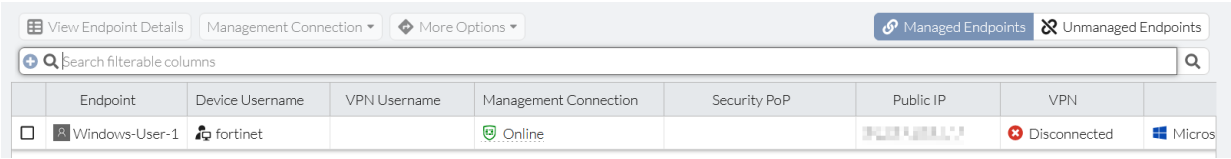
Example: Adding an endpoint to management after it was previously removed

To add an endpoint to management after it was previously removed:

1. Consider that the device has been unmanaged and previously removed from management. Go to *Network* > *Managed Endpoints*, click the *Unmanaged Endpoints* view and confirm the endpoint is visible there.
2. Select the endpoint, select *Management Connection* > *Enable*, and click *OK* to confirm.



3. Go to *Configuration* > *Users* and click *Onboard Users*.
4. Set *FortiClient Installer* to *Download*.
5. Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
6. On the endpoint, open FortiClient. On the *Zero Trust Telemetry* tab, paste the copied FortiSASE invitation code and click *Connect*. The endpoint successfully establishes a zero trust telemetry connection with FortiSASE. Upon connection, FortiClient receives an endpoint policy from FortiSASE. A system tray bubble message displays once the download completes.
7. Go to *Network* > *Managed Endpoints* and click *Managed Endpoints*. Confirm the endpoint is visible in that view and that the *Management Connection* is *Online*. If the endpoint reboots, it continues to establish its zero trust telemetry connection with FortiSASE and receives an endpoint policy each time.



Digital Experience

Digital experience monitoring (DEM) serves as a valuable tool for network administrators in diagnosing connectivity and network issues for remote users along with monitoring their real-time network bandwidth, CPU, memory, and hard disk usage. It also enables tracing end-to-end network performance, from an endpoint to a FortiSASE PoP and to a SaaS application using a DEM agent installed on the endpoint. DEM provides insights into potential network issues between a FortiClient endpoint, FortiSASE PoP, SaaS applications, and the internet service providers (ISP) connecting them.

DEM requires an Advanced remote users FortiSASE license or a Comprehensive remote users FortiSASE license. See the SASE and Zero Trust Ordering Guide. It also requires installing the DEM agent on endpoints.

For new FortiSASE instances with an Advanced or Comprehensive license, the DEM agent is packaged along with the FortiClient installer and available to download as a single executable file from FortiSASE when users download FortiClient. See Managed endpoint client onboarding on page 285.

For existing FortiSASE instances with an Advanced or Comprehensive license, endpoint users are prompted to begin upgrading to a FortiClient version that supports the DEM agent and the DEM agent is installed automatically during this upgrade.

To uninstall the DEM agent, do the following:

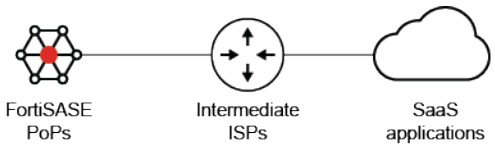
- On macOS, use the uninstaller tool to uninstall FortiClient and the DEM agent together.
- On Windows, use the installer package to uninstall FortiClient and the DEM agent together. You cannot uninstall DEM agent using *Add* or *Remove Program* in Control Panel.

To navigate DEM:

1. Go to *Network* > *Managed endpoints* to see the list of managed and unmanaged endpoints.
2. Select an endpoint and click *View Endpoint Details*. A new slide in appears and the following endpoint details are visible:

GUI option	Description
Details	Shows general endpoint information such as the hostname, management connection to FortiSASE, and VPN status. See Managed Endpoints on page 120. DEM displays information on all detected network interfaces and their IP addresses, and a real-time network bandwidth graph that shows total bandwidth used by endpoint.
Hardware	Shows information regarding endpoint hardware such as vendor, model, and CPU. It displays a real-time graph that shows total hard disk, CPU, and memory usage on the endpoint.
Digital Experience	1. Shows DEM agent status: offline, online, or agent is not installed. To get end-to-end network performance visibility from the endpoint to a particular SaaS application, run a trace job for the selected endpoint. SeeTo run a trace job on an endpoint: on page 126.

DEM displays a list of SaaS applications and health check metrics for first-mile connectivity between the geographical PoPs provisioned for your FortiSASE instance and SaaS applications, as the following diagram shows. See Digital Experience Monitoring on page 128.



Running a trace job on an endpoint

FortiSASE can run a trace job on the endpoint using DEM agent. This assists in troubleshooting various performance bottlenecks in the network by providing link metrics such as average RTT and packet loss on various hops of the network.

To run a trace job on an endpoint:

1. Go to *Network* > *Managed Endpoints*.
2. Select the desired endpoint and click *View Endpoint Details*. A slide in appears.
3. In the *Digital Experience* column, the *DEM agent status* must be *Online*. From the *SaaS application* dropdown list, select an application to test the connection to from the selected endpoint.
4. Under *Monitor for*, configure a suitable time to run the trace job for the specified duration.
5. Click *Start* to schedule the job.

If you interrupt the current running job by clicking *Stop*, FortiSASE deletes the historical traceroute data collected so far and you must restart the job.

The first trace job output displays within five minutes after clicking *Start*, after which FortiSASE presents output every three minutes until the selected *Monitor for* duration expires. FortiSASE stores the results displayed for three days only for the latest trace job. To analyze the trace job, see Analyzing trace job result on page 126.

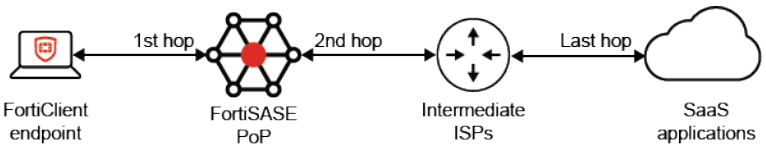
To run the trace job, the following must be true:

- DEM agent is installed on endpoint.
- *DEM agent status* must be *Online* under *Digital Experience* tab under *Network* > *Managed Endpoints*> *View Endpoint Details* for selected endpoint.
- Application Control security profile and internet access firewall policy must not block ping or ICMP traffic.

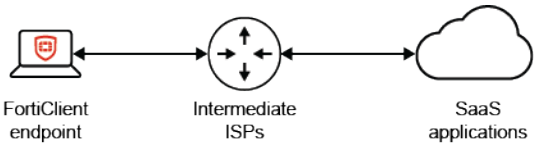
Analyzing trace job result

The trace job output gives information on average RTT (ms) and packet loss (%) on various hops of the network. To identify the hop accurately, understanding whether the selected endpoint is connected to the FortiSASE VPN tunnel for secure internet access (SIA) or not is important.

When an endpoint is connected to the FortiSASE VPN tunnel, it accesses SaaS applications using SIA. Thus, the first and second hops of the trace are the entry and exit interface IP address of the FortiSASE PoP that the endpoint is connected to. The remaining hops are the ISPs in between until the last hop, which is the selected SaaS application.



When an endpoint is not connected to the FortiSASE tunnel, it accesses SaaS applications directly using its local internet breakout bypassing the FortiSASE PoP. Thus, the performance metrics (average RTT and packet loss) displayed do not include the FortiSASE PoP.



Some ISPs do not respond to the trace packets that the DEM agent sends and requests time out. For such hops, their entry is marked as *** in the trace result output.

Each FortiSASE administrator can only run one trace job on unique endpoints simultaneously.

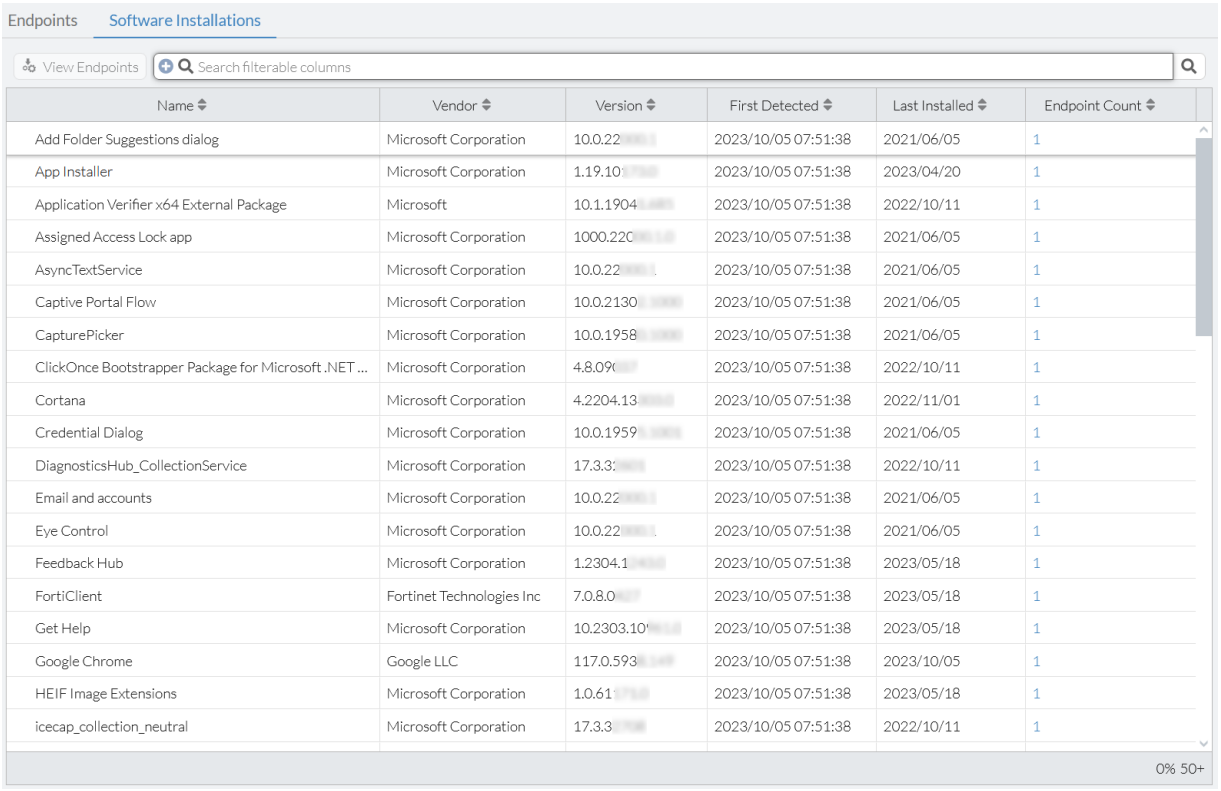
Application inventory for managed endpoints

You may want to view which applications have been installed on FortiSASE managed endpoints.

For managed endpoints, FortiClient sends the software inventory information to FortiSASE when it first registers to FortiSASE. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to FortiSASE.

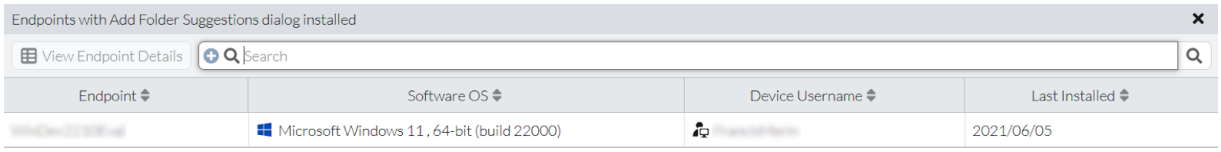
Based on this information sent by FortiClient, you can view the application inventory for FortiSASE managed endpoints as follows:

- Go to *Network* > *Managed Endpoints* and select the *Software Installations* tab to view a global list of applications installed on all endpoints.
  - The *Endpoint Count* field displays the number of endpoints with the specific application installed.

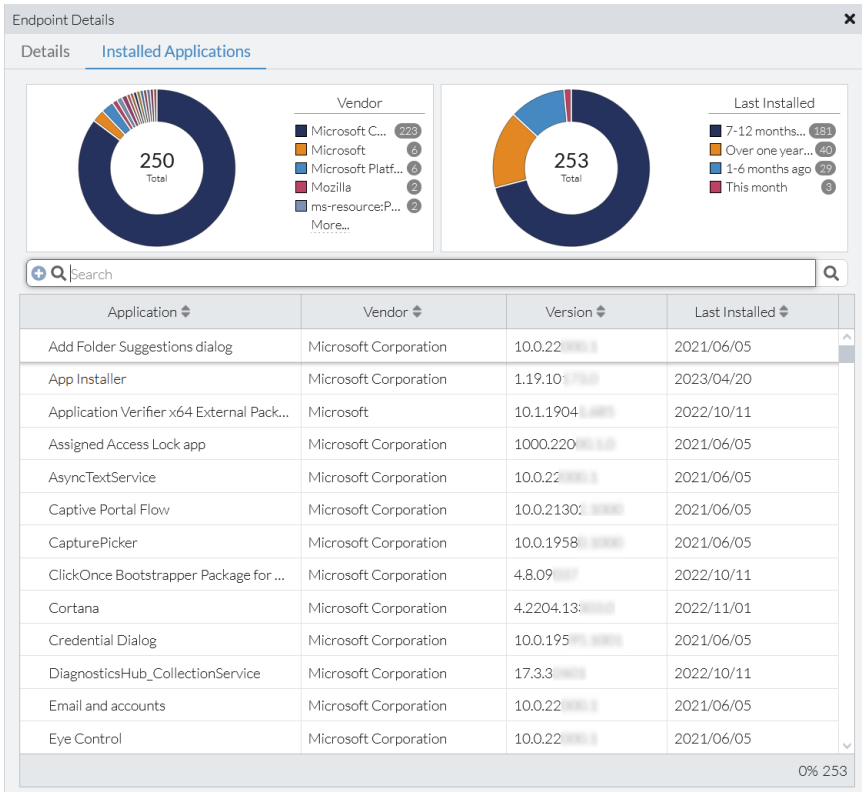


  - You can select an application and either click *View Endpoints* or right-click and select *View Endpoints* to view

which endpoints have the application installed.



- Go to *Network* > *Managed Endpoints*, select the *Endpoints* tab, select an endpoint, and either click *View Endpoints Details* or right-click and select *View Endpoint Details*. From the *Endpoint Details* pane, click *Installed Applications* to view a list of installed applications for the selected endpoint.



Each list includes details for each application such as vendor and version information.

Digital Experience Monitoring

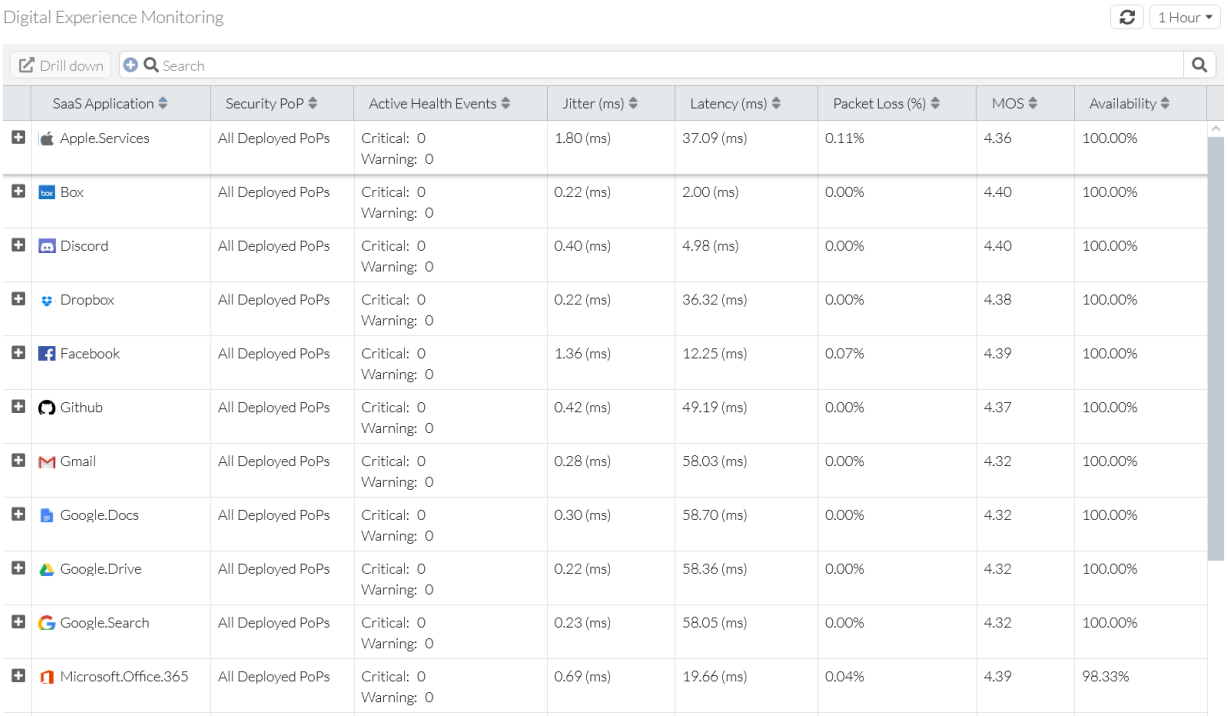
To assist network administrators with troubleshooting remote user connectivity issues to common SaaS applications, FortiSASE includes a digital experience monitoring (DEM) page accessible from *Network* > *Digital Experience Monitoring*.

You can also add a *Digital Experience Monitoring* widget to *Dashboards* > *Status*.

To monitor end-to-end network performance from an endpoint to a FortiSASE PoP and to a SaaS application, see Digital Experience on page 124.

To be configurable, the DEM feature requires either an Advanced remote users FortiSASE license or a Comprehensive remote users FortiSASE license. See the FortiSASE Ordering Guide.

Network > *Digital Experience Monitoring* displays a list of SaaS applications and health check metrics for first-mile connectivity between the geographical points of presence (PoPs) provisioned for your FortiSASE instance and these SaaS applications. An administrator can use this information to determine if remote user traffic is passing through a PoP with ideal connectivity or with some ongoing connectivity issues.



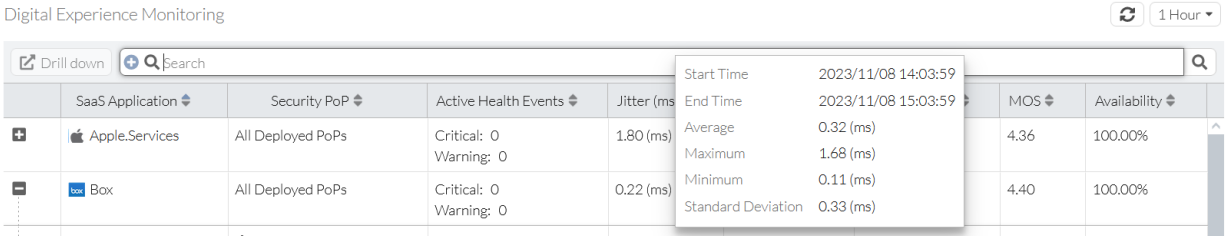
SaaS Application	Security PoP	Active Health Events	Jitter (ms)	Latency (ms)	Packet Loss (%)	MOS	Availability
Apple.Services	All Deployed PoPs	Critical: 0 Warning: 0	1.80 (ms)	37.09 (ms)	0.11%	4.36	100.00%
Box	All Deployed PoPs	Critical: 0 Warning: 0	0.22 (ms)	2.00 (ms)	0.00%	4.40	100.00%
Discord	All Deployed PoPs	Critical: 0 Warning: 0	0.40 (ms)	4.98 (ms)	0.00%	4.40	100.00%
Dropbox	All Deployed PoPs	Critical: 0 Warning: 0	0.22 (ms)	36.32 (ms)	0.00%	4.38	100.00%
Facebook	All Deployed PoPs	Critical: 0 Warning: 0	1.36 (ms)	12.25 (ms)	0.07%	4.39	100.00%
Github	All Deployed PoPs	Critical: 0 Warning: 0	0.42 (ms)	49.19 (ms)	0.00%	4.37	100.00%
Gmail	All Deployed PoPs	Critical: 0 Warning: 0	0.28 (ms)	58.03 (ms)	0.00%	4.32	100.00%
Google.Docs	All Deployed PoPs	Critical: 0 Warning: 0	0.30 (ms)	58.70 (ms)	0.00%	4.32	100.00%
Google.Drive	All Deployed PoPs	Critical: 0 Warning: 0	0.22 (ms)	58.36 (ms)	0.00%	4.32	100.00%
Google.Search	All Deployed PoPs	Critical: 0 Warning: 0	0.23 (ms)	58.05 (ms)	0.00%	4.32	100.00%
Microsoft.Office.365	All Deployed PoPs	Critical: 0 Warning: 0	0.69 (ms)	19.66 (ms)	0.04%	4.39	98.33%

Digital Experience Monitoring displays historic data that you can filter by the following durations:

- One hour (default)
- One day
- One week
- One month
- One year

You can also refresh data for the selected time duration.

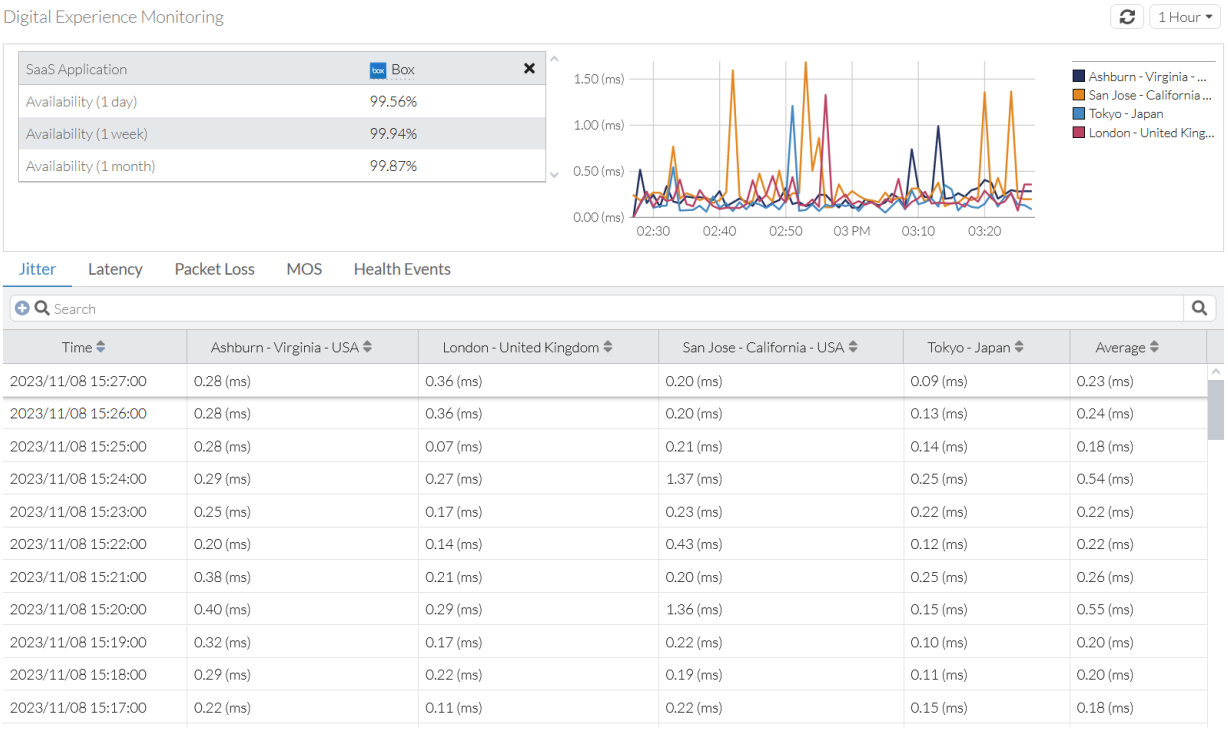
You can view more details for each metric by hovering the mouse over a metric to display tooltips.



You can view more details for a specific SaaS application using one of these methods:

- Selecting an application and clicking *Drill down*
- Double-clicking an entry
- Right-clicking while an application is selected and selecting the drilldown option

The drilldown page provides more detail for the time duration selected in the form of charts and tables.



From the main or the drilldown page, you can perform the following operations:

- *Best Fit Columns*
- *Reset Table*
- *Export* displayed data to a file in CSV or JSON format
- *Select Columns*

Requesting FortiClient diagnostic logs from endpoints

This feature only works with Windows endpoints that fulfill the following criteria:

- Running FortiClient
- Online
- Managed by FortiSASE Endpoint Management Service

FortiSASE supports requesting the export of FortiClient diagnostic logs on-demand from a single online Windows endpoint from one of the following:

- *Details* tab in *View Endpoint Details*
- *More options* in the *Endpoints* tab in *Managed Endpoints*

Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes. When new logs are generated, then the old ones will be overwritten.

To request FortiClient diagnostic logs from an endpoint:

1. Go to *Network* > *Managed Endpoints*.
2. Select a Windows endpoint that is online and perform one of these steps:
   - Click *View Endpoint Details* and in the *Details* tab, next to the *Diagnostic Logs* field, click *Request new logs*.
   - Click *More Options* > *Export Diagnostic Logs* and in the *Export diagnostic logs* prompt, click *Request new logs*.
3. In the top right, observe the notification *Successfully requested diagnostic logs from the endpoint* displays, indicating that FortiSASE sent the request successfully.

To download previously requested FortiClient diagnostic logs from an endpoint:

1. Go to *Network* > *Managed Endpoints*.
2. Select a Windows endpoint that you previously sent a log request to and perform one of these steps:
   - Click *View Endpoint Details* and in the *Details* tab, next to the *Diagnostic Logs* field, click *Download* to download the available diagnostic logs for the endpoint.
   - Click *More Options* > *Export Diagnostic Logs* and in the *Export diagnostic logs* prompt, click *Download* to download the available diagnostic logs for the endpoint.

Configuration

DNS Settings

The *DNS Server* setting in FortiSASE under *Configuration* > *DNS* is used by remote users to resolve hostnames for both internal and external domains.

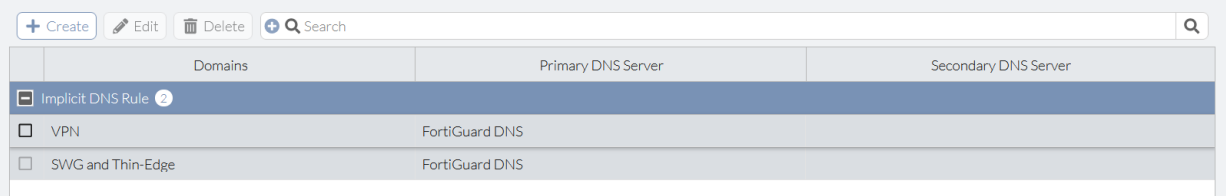
- Implicit DNS rules have been predefined for VPN users and for SWG and Thin-Edge users. These are used for resolving hostnames for external domains.
- Split DNS rules can be created by clicking on the *Create* button. These are used for resolving hostnames for internal domains. See Split DNS Rules on page 134.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.



By default, FortiSASE deployments use FortiGuard DNS as the default DNS server for implicit DNS rules. You can select any implicit DNS rule and click *Edit* to change the default DNS server.

FortiGuard DNS servers do not support DNS over TCP. If you require DNS over TCP, edit implicit DNS rules from the default FortiGuard DNS server to other DNS servers that support DNS over TCP.

You can configure *Default DNS Server* with one of the following options, then click *OK* to save the change:

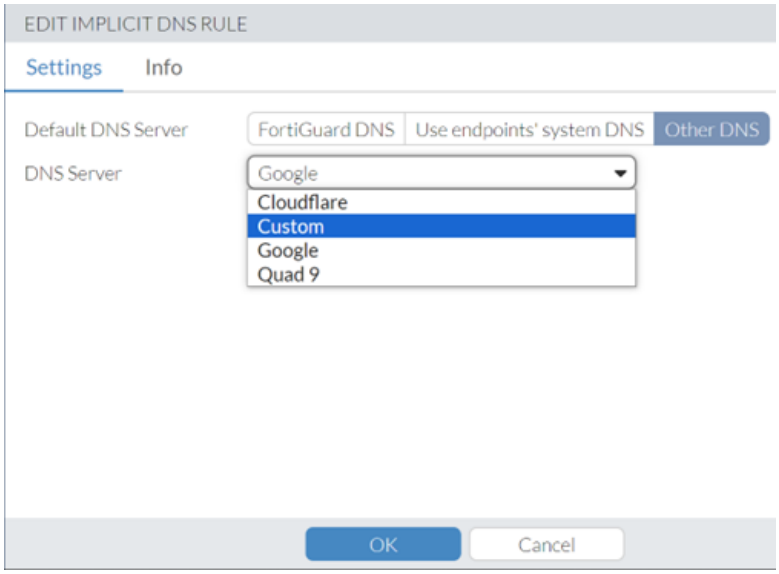
DNS Server	Description	Primary and Secondary DNS Server IP Address
FortiGuard DNS	Use FortiGuard DNS	96.45.45.45

DNS Server	Description	Primary and Secondary DNS Server IP Address
		96.45.45.46
Use endpoints' system DNS	Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS	Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
CloudFlare	Use the CloudFlare public DNS server	1.1.1.1 1.0.0.1
Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify IP address of primary and secondary DNS.
Google	Use the Google public DNS server	8.8.8.8 8.8.4.4
Quad 9	Use the Quad 9 public DNS server	9.9.9.9 149.112.112.112

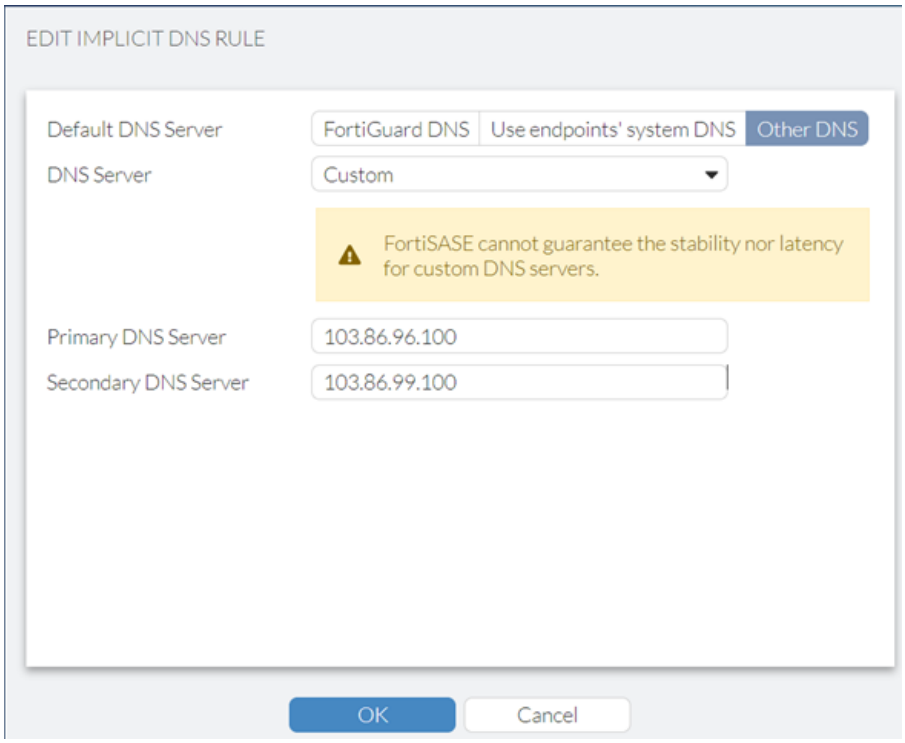
For example, you can edit the VPN implicit DNS rule to use a custom DNS server as follows:

To configure a custom DNS server:

1. Go to *Configuration* > *DNS*, select *VPN Implicit DNS Rule*, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.
3. From the *DNS Server* dropdown, select *Custom*.



4. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the respective IP addresses for the servers of your choice.



5. Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most secure internet access (SIA) use cases that simply require remote users to resolve hostnames for external domains.

Split DNS Rules

FortiSASE users will often need to resolve internal hostnames that are not resolvable by public DNS servers in scenarios including but not limited to:

- When agent-based users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server.
- When agent-based, agentless, or site-based FortiExtender users are located remotely, FortiSASE Private Access has been configured with Secure Private Access (SPA) hubs, and users must use an internal DNS server behind the SPA hub.

To support these scenarios, FortiSASE DNS settings can be configured for split DNS using *Split DNS Rules*.

Split DNS works as follows:

- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s).
- Resolve all other hostnames for external domains using the implicit DNS rule.

Split DNS is more efficient than sending all DNS requests to internal DNS servers because it reduces any potential latency and downtime with using internal DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource internal DNS server deployments. For resolving hostnames for external domains, split DNS leverages the redundancy, extensive resources, and geographical coverage of public DNS servers with anycast capabilities.

For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE will yield inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

To secure DNS requests, the DNS-over-HTTPS (DoH) protocol secures DNS requests and replies sent and received over HTTPS and works with public DNS servers that support this protocol. DoH is enabled by default on modern web browsers including Chrome, Edge, and Firefox and is supported by Google's public DNS servers, which is the default for upgraded FortiSASE deployments. Therefore, for split DNS rules to work with DNS servers that support DoH, SSL deep inspection must be enabled for agent-based remote users on FortiSASE.

Prerequisites

SSL Deep Inspection

Split DNS requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept the DNS traffic.

- To confirm SSL deep inspection is enabled, go to *Configuration* > *Security* and under the *SSL Inspection* widget ensure *Deep Inspection* is displayed.
- To enable SSL deep inspection, go to *Configuration* > *Security* and in the *SSL Inspection* widget click on *Customize*. In the *SSL Inspection* pane, select *Deep Inspection* and click *OK*.

See Certificate and deep inspection modes on page 146 for further details on deep inspection.

Install FortiSASE CA Certificate for Agentless and Site-based FortiExtender Users

With deep inspection enabled, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing Certificate Authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints.

The FortiSASE CA certificate must be manually installed on endpoints for agentless SWG users and site-based FortiExtender users.

- For agentless SWG users, installing this CA certificate is already part of the SWG onboarding process.
- For endpoints using a site-based FortiExtender, installing this CA certificate is an additional step that must be performed.

See Certificate installation on page 291 for installing the FortiSASE CA certificate. Although these steps are geared toward onboarding SWG users, they also apply for site-based FortiExtender users.

Access to Internal DNS Server

Ensure that your FortiSASE remote users have access to the internal DNS server.

For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE will yield inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

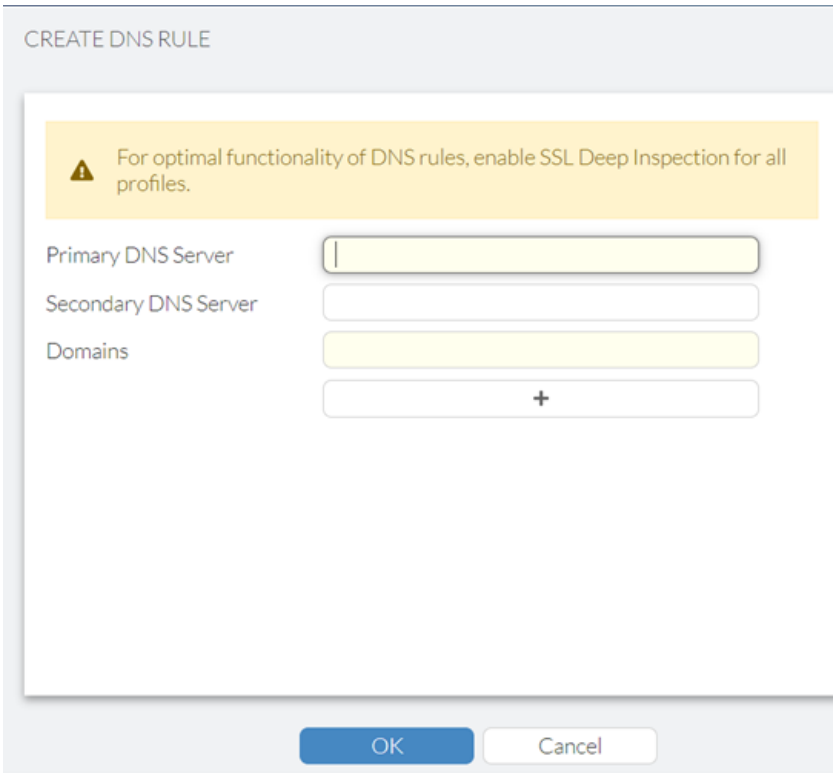
When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

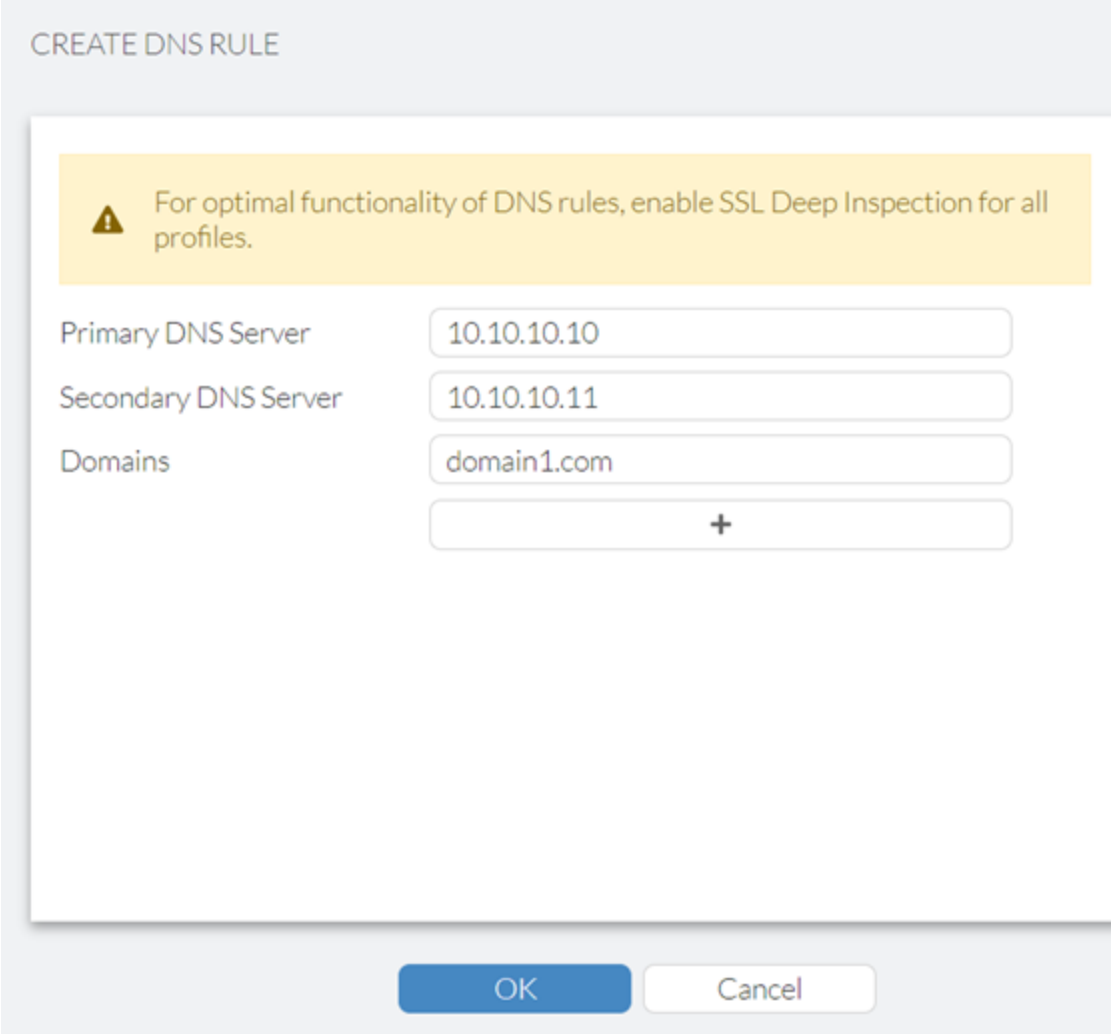
Configuring Split DNS Rules

To configure Split DNS Rules:

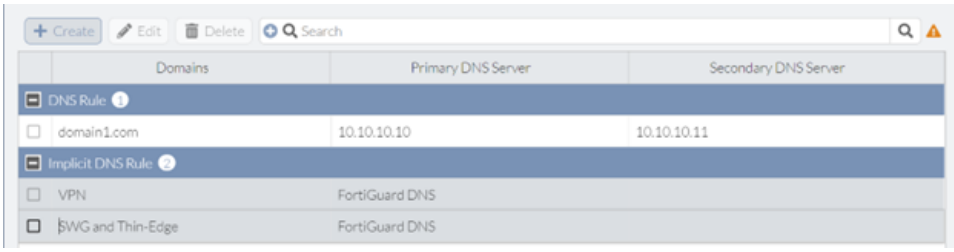
1. Go to *Configuration* > *DNS*.
2. Click *Create*.



3. In the *Create DNS Rule* pane, enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*. Click + to add more fields to enter in additional domains. Click *OK*.



4. Observe that the split DNS rule has been created and is displayed in the table.



If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.

If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

Policies

You must associate any traffic going through FortiSASE with a policy. Policies control where the traffic goes, how FortiSASE processes it, and whether or not FortiSASE allows it to pass through.

When a session is initiated through the VPN tunnel, FortiSASE analyzes the connection and performs a VPN policy match. FortiSASE performs the match from top down and compares the session with the configured VPN policy parameters. When there is a match and the action is *Accept*, FortiSASE applies the enabled security components to the traffic. If the action is *Deny*, FortiSASE blocks the traffic from proceeding.

Default VPN policies

FortiSASE is configured with the following default VPN policies:

VPN policy	Description
Allow-All	Allows traffic for all services for all VPN users. You can edit and delete this VPN policy.
Implicit Deny	Denies access to traffic that does not match another configured VPN policy. You cannot edit or delete this VPN policy.

With only these default VPN policies and no custom configurations, FortiSASE allows traffic to pass through the Allow-All VPN policy, and applies the enabled security components for scanning and processing.

Adding policies to perform granular firewall actions and inspection

You can add multiple policies to perform granular firewall actions and inspection. This example configures a policy to allow a set of remote users to access *.fortinet.com and blocks the same remote users from accessing all traffic to *.netflix.com.

Policy name	Description
RemoteHomeOffice-DenyNetflix	Blocks remote employees (members of the Remote-Home-Office VPN user group) from accessing *.netflix.com.
RemoteHomeOffice-AllowFortinet	Allows remote employees (members of the Remote-Home-Office VPN user group) to access *.fortinet.com.

The following provides instructions for configuring the described policies. You may want to configure similar policies, modifying settings based on your environment.

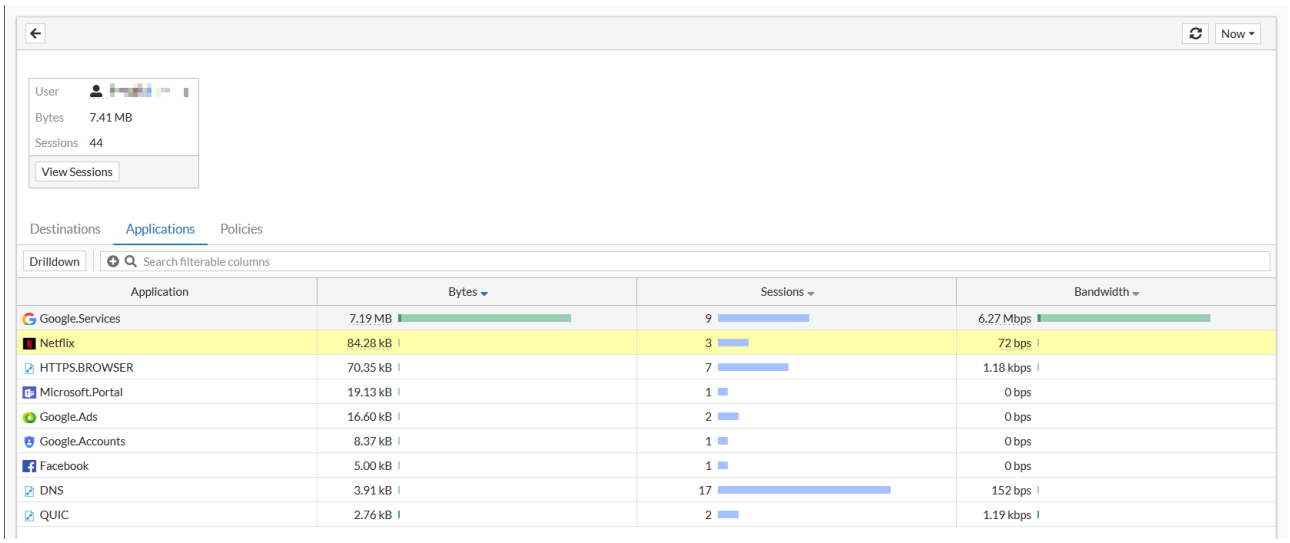
To add policies to perform granular firewall actions and inspection:

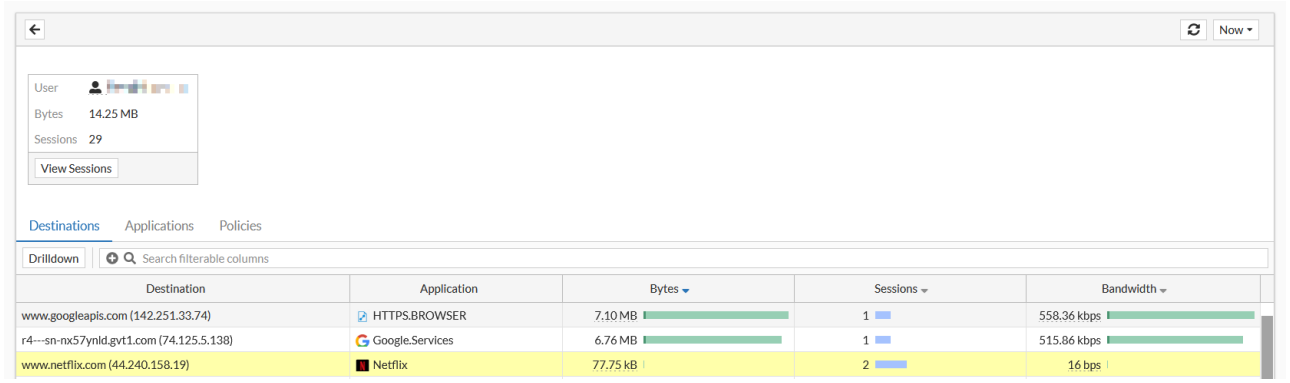
1. Go to *Configuration* > *Policies*.
2. Create the RemoteHomeOffice-DenyNetflix policy:
   a. Click *Create*.
   b. For *Source Scope*, select *VPN Users*.
   c. For *User*, select *Specify*: Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.

   d. In the *Destination* field, select *Specify*, click +, then do the following:
      i. On the *Host* tab, click *Create*.
      ii. Select *IPv4 Host*.
      iii. In the *Name* field, enter the desired name.
      iv. From the *Type* dropdown list, select *FQDN*.
      v. In the *FQDN* field, enter *.netflix.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
      vi. Click *OK*.
      vii. Select the newly created Netflix host.
   e. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
   f. Leave all other fields at their default values.
   g. Click *OK*.
3. Create the RemoteHomeOffice-AllowFortinet policy:
   a. Click *Create*.
   b. For *User*, select *Specify*. Click +, and select the *Remote-Home-Office* user group from the *Select Entries* pane.
   c. In the *Destination* field, click +, then do the following:
      i. On the *Host* tab, click *Create*.
      ii. Select *IPv4 Host*.
      iii. In the *Name* field, enter the desired name.
      iv. From the *Type* dropdown list, select *FQDN*.
      v. In the *FQDN* field, enter *.fortinet.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.
      vi. Click *OK*.
      vii. Select the newly created Fortinet host.
   d. In the *Service* field, click +. On the *Select Entries* pane, select *ALL*.
   e. For *Action*, select *Accept*.
   f. Leave all other fields at their default values.
   g. Click *OK*.
4. In *Configuration* > *Policies*, ensure that you order the policies so that RemoteHomeOffice-DenyNetflix policy is before the RemoteHomeOffice-AllowFortinet policy, and that both those VPN policies are before the Allow-All policy.

When a session is initiated through the VPN tunnel, FortiSASE analyzes the connection and performs a policy match. FortiSASE performs the match from top down and compares the session with the configured policy parameters. For example, consider that a user who belongs to the Remote-Home-Office user group attempts to access www.fortinet.com. FortiSASE attempts to match the RemoteHomeOffice-DenyNetflix, but the traffic is not for *.netflix.com. Then, FortiSASE attempts to match the next policy, the RemoteHomeOffice-AllowFortinet policy, which matches. FortiSASE allows the user access to www.fortinet.com.

You can view data for access attempts on the FortiView Sources dashboard. You can view the application, destination, and policy information.





Configuring a policy to allow traffic from an Edge device to FortiSASE

To configure a policy to allow traffic from an Edge device to FortiSASE for internet access:

1. Go to *Configuration* > *Policies*.
2. On the *Internet Access* tab, click *+Create* to create a new policy.

3. Configure these fields:

Field	Value
Name	Enter a unique internet access policy name.
Source Scope	• *All*: all FortiSASE users/devices • *VPN Users*: remote endpoint users • *Edge Devices*: edge devices such as FortiExtender • *Specify*: specify selected hosts and host groups if you selected *VPN Users*, or authorized Edge devices if you selected *Edge Devices*.
Destination	• *All Internet Traffic*: all internet access traffic • *Specify*: specify selected internet access hosts or host groups
Service	Click + and select entries.
Action	*Accept* or *Deny*.
Profile Group	*Default* or *Specify* and select profile group.
Force Certificate Inspection	Enable or disable. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead use certificate inspection.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • *Security Events*: log traffic that has a security profile applied to it. • *All Sessions*: log all sessions that this policy accepts or denies.

4. Click *OK*.

To configure a policy to allow traffic from an Edge device to FortiSASE for private access:

See Configuring a private access policy for remote VPN users and edge devices on page 102.

SWG Policies

You must associate any traffic going through FortiSASE with a policy. Secure web gateway (SWG) policies control where the traffic goes, how FortiSASE processes it, and whether or not FortiSASE allows it to pass through.

When a user's client software, such as a web browser, proxies traffic through FortiSASE, FortiSASE analyzes the connection and performs a SWG policy match. FortiSASE performs the match from top down and compares the session with the configured policy parameters. When there is a match and the action is *Accept*, FortiSASE applies the enabled security components to the traffic. If the action is *Deny*, FortiSASE blocks the traffic from proceeding.

You must first enable SWG configuration for the feature to be available in the GUI. See SWG Configuration on page 270.

Default SWG policies

FortiSASE is configured with the following default secure web gateway (SWG) policies:

SWG policy	Description
DENY_BOTNET	Denies traffic to known botnet C&C servers for all SWG users. You cannot edit or delete this SWG policy.
Allow-All	Allows traffic for all services for all SWG users. You can edit and delete this SWG policy.
Implicit Deny	Denies access to traffic that does not match another configured SWG policy. You cannot edit or delete this SWG policy.

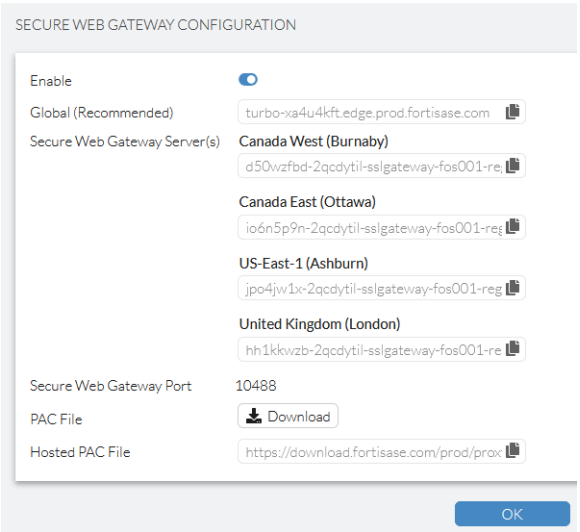
With only these default SWG policies and no custom configurations, FortiSASE blocks all traffic to known botnet C&C servers, allows all other traffic to pass through the Allow-All SWG policy, and applies the enabled security components for scanning and processing.

Configuring a SWG policy

This example configures a secure web gateway (SWG) policy to block all SWG users from accessing all traffic to *.netflix.com.

To configure an SWG policy:

1. Enable SWG configuration:
   a. Go to *System* > *SWG Configuration*.
   b. Toggle *Enable* to on. The GUI may take a few minutes to reload. Once the GUI finishes loading, you can view the *Hosted PAC File* field. Endpoint users use this URL to configure connecting via the FortiSASE SWG server.



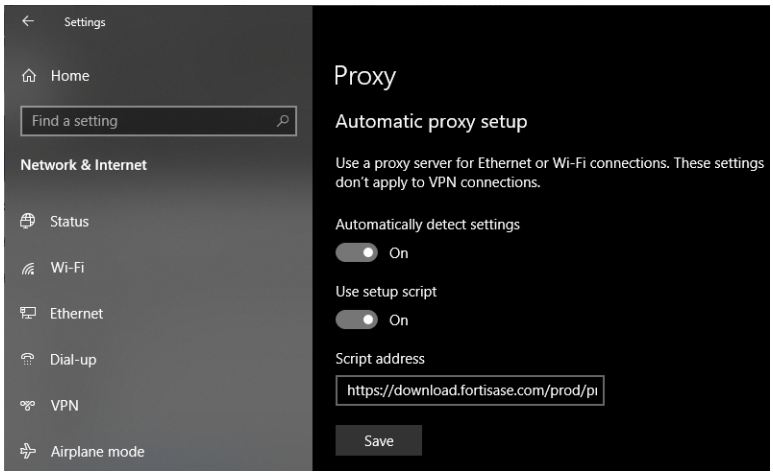
   c. On the right pane, click *Download SWG Certificates*. You must distribute this certificate to end users to install on their endpoints to avoid untrusted certificate errors.
2. Create the SWG-DenyNetflix SWG policy:
   a. Go to *Configuration* > *SWG Policies*.
   b. Click *Create*.

c. Configure the SWG-DenyNetflix SWG policy:
   i. For *User*, select *All SWG Users*.
   ii. In the *Destination* field, click *Specify*.
   iii. On the *Host* tab, click *Create*.
   iv. Select *IPv4 Host*. Configure the fields as follows:

Field	Value
Name	Enter the desired name.
Type	i. Select *FQDN*.
FQDN	Enter *.netflix.com. When using wildcard FQDNs, FortiSASE caches the FQDN address's IP addresses based on matching DNS responses.

   v. Click *OK*.
   vi. Select the newly created Netflix host.
   vii. In the *Service* field, click +. On the *Select Entries* pane, select *webSWG*.
   viii. Leave all other fields at their default values.
   ix. Click *OK*.

3. In *Configuration* > *SWG Policies*, ensure that you order the policies so that the SWG-DenyNetflix policy is before the Allow-All policy.
4. Distribute the URL in the *System* > *SWG Configuration* > *Hosted PAC File* field and the certificate downloaded from *Download SWG Certificates* to end users.
5. The end user installs the certificate on their device.
6. The end user can configure SWG settings at the OS level or in a browser. Configuring SWG settings at the OS level applies them to all installed browsers. The following gives instructions for configuring SWG settings at the OS level on a Windows 10 device:
   a. In Windows, go to *Windows Settings* > *System* > *SWG Settings*.
   b. Enable *Use setup script*.
   c. In the *Script address* field, enter the *Hosted PAC File* URL.



   d. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

When a session is initiated through the client browser, FortiSASE analyzes the connection and performs an SWG policy match. FortiSASE performs the match from top down and compares the session with the configured SWG policy

parameters. For example, consider that an SWG user attempts to access www.netflix.com. FortiSASE attempts to match the SWG-DenyNetflix policy, which matches. FortiSASE denies the user access to www.netflix.com.

Security

You can configure FortiSASE security components settings and view logs for each component in *Security*. FortiSASE applies enabled security components to each Allow policy in *Policies*. You can configure some exemptions and overrides for some security components.

Decrypting and inspecting content in encrypted traffic for these FortiSASE security features requires deep inspection:

- Antivirus
- Web Filtering with Inline-CASB
- File Filter
- Data loss prevention
- Application Control with Inline-CASB

Without deep inspection configured on FortiSASE and the corresponding certificate authority (CA) certificate automatically installed on the endpoint with FortiClient, the aforementioned features do not work as desired with encrypted traffic.

See Certificate and deep inspection modes on page 146.

Security profile groups

You can create security profile groups, which allow you to group different security profile settings together. You can then configure the profile group as part of a policy.

For example, consider the RemoteHomeOffice-AllowFortinet example policy from Adding policies to perform granular firewall actions and inspection on page 139, which allows remote employees (members of the Remote-Home-Office VPN user group) to access *.fortinet.com. Consider that you also want to monitor these employees' access to Cloud/IT applications using Application Control With Inline-CASB, while disabling Application Control With Inline-CASB for all other employees. You can achieve this by creating a new security profile group with the desired Application Control With Inline-CASB settings, and configuring this profile group as part of the RemoteHomeOffice-AllowFortinet policy. Application Control With Inline-CASB remains disabled for policies that have another security profile group applied.

The following provides for configuring the described scenario.

To create a security profile group and configure it in a policy:

1. Go to *Configuration* > *Security*. By default, the *Internet Access* tab is selected in the top right corner.

If you have configured secure private access, you can select between the *Internet Access* or *Private Access* tabs to select which traffic the security profile group applies to.

Currently, when a security profile group is configured for *Private Access*, it applies to private access traffic in both directions, that is, in the *To hubs* and the *From hubs* directions.

2. From the *Profile Group* dropdown list in the top right corner, click *Create*.

3. In the *Name* field, enter the desired name. This example uses "Cloud IT" as the group name.
4. In the *Initial Configuration* field, do one of the following:
   a. Select *Default* to configure the new group with the same settings as the default security profile group.
   b. Select *Based On* to configure the new group with the same settings as an existing non-default security profile group. From the dropdown list, select the desired group.
5. Click *OK*.
6. Configure Application Control With Inline-CASB to monitor employees' access of Cloud/IT applications by enabling Application Control With Inline-CASB. By default, once enabled, Application Control With Inline-CASB monitors access of Cloud/IT applications.
7. Configure the profile group in a policy:
   a. Go to *Configuration* > *VPN Policies*.
   b. Select the RemoteHomeOffice-AllowFortinet policy.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select *Cloud IT*. The *Profile Group* field is only available for policies where the *Action* is configured as *Accept*.
   d. Click *OK*.

SSL Inspection

Secure sockets layer (SSL) inspection allows FortiSASE to inspect the SSL/TLS layer during certificate inspection and upper layers during deep inspection. This enables FortiSASE to filter and protect secured traffic that the various security profiles have processed. SSL inspection not only protects traffic over HTTPS, but also from other commonly used encrypted protocols such as SMTPS, POP3S, IMAPS, and FTPS. FortiSASE supports two SSL inspection types.

Certificate and deep inspection modes

These FortiSASE features require deep inspection to decrypt and inspect content in encrypted traffic:

- Split DNS
- Antivirus
- Web Filtering with Inline-CASB
- File Filter
- Data loss prevention
- Application Control with Inline-CASB

Without deep inspection configured on FortiSASE and the corresponding certificate authority (CA) certificate automatically installed on the endpoint with FortiClient, the aforementioned features do not work as desired with encrypted traffic.

You can configure FortiSASE SSL inspection to use certificate (default) or deep inspection, or disable SSL inspection altogether.

Mode	Description
Certificate inspection	FortiSASE inspects only the header information up to the SSL/TLS layer. Certificate inspection verifies the web server identities by analyzing the SSL/TLS negotiations by looking at the server certificate and TLS connection parameters. Therefore web filter can perform FortiGuard category web filtering, URL filtering, and other filtering that does not require looking at the payload when you enable certificate inspection.
Deep inspection	FortiSASE decrypts and inspects the content to find and block threats. It then reencrypts the content and sends it to the real recipient. You can configure exemptions for deep inspection. While HTTPS offers protection on the internet by applying SSL encryption to web traffic, malicious traffic can also use SSL encryption to get around your network's normal defenses. For example, you may download a file containing a virus during an e-commerce session or receive a phishing email containing a seemingly harmless download that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer. You can use SSL inspection to protect the infiltration by scanning for malicious content in your HTTPS web traffic or identifying phishing content in encrypted mail exchanges. SSL inspection can also defend against the exfiltration process while an infected host calls home to a C&C server or leaks company secrets over encrypted sessions. When you use deep inspection, FortiSASE serves as the intermediary to connect to the SSL server. It decrypts and inspect the content to find threats and block them. The recipient is presented with the FortiSASE certificate or a custom certificate instead of the real server certificate. FortiClient receives the certificate automatically and endpoint users do not see any certificate browser warnings.
No inspection	FortiSASE does not perform any SSL inspection. You can use this option to fully disable SSL inspection.

Exempting hosts and URL categories from deep inspection

In some scenarios, you may not want to perform SSL deep inspection and simply choose to trust the connections or the user initiating the connections. In this case, certificates of the hosts and URL categories are inspected but contents are not decrypted for inspection. Thus, security scanning of encrypted traffic for exempted hosts and websites matching exempted URL categories are not performed.

For example, for banking-related traffic, most end users do not want deep inspection applied out of privacy reasons. Similarly, traffic related to personal health and wellness may contain personal information that is too sensitive to scan. As such, when defining deep inspection, FortiSASE exempts the Finance and Banking and Health and Wellness categories by default.

In other cases, a user or user group may need to access websites without deep inspection. Exempting a host or hosts associated with a user or user group achieves this result.

To exempt hosts and URL categories from deep inspection:

1. Go to *Configuration* > *Security*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Customize*.
3. Enable *Deep Inspection*.
4. In the *Hosts* and *URL Categories* fields, click +.
5. In the *Select Entries* pane, select the desired hosts and URL categories to exempt from deep inspection.
6. Click *OK*.

Uploading a certificate for deep inspection mode

By default, you can download the certificate authority (CA) certificate of the FortiSASE CA, Fortinet_CA_SSL, who signs the certificate used in encrypting SSL connections when performing deep inspection. If desired, you can upload a custom CA certificate and key to perform deep inspection.

To upload a certificate for deep inspection mode:

1. Go to *Configuration* > *Security*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Customize*.
3. Enable *Deep Inspection*.
4. From the *CA Certificate* dropdown list, select + to import a new local CA certificate and key for use with deep inspection.
5. Configure the fields and upload the certificate and key files as needed.
6. Click *OK*.

Installing a certificate for deep inspection mode

When users forward traffic to FortiSASE using agent-based mode, agentless secure web gateway (SWG) mode, or using an edge device, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

With deep inspection enabled, FortiSASE supports automatically installing the FortiSASE CA certificate for agent-based users with FortiClient installed on their endpoints. Therefore, the following instructions are not required for agent-based users.

You must install the FortiSASE CA certificate on endpoints for agentless SWG users and site-based edge device users using the instructions below.

The following instructions demonstrate installing certificates on various operating systems:

- Windows on page 149
- macOS on page 149
- Chrome OS on page 150
- Managed Chromebook on page 150

First, you will need to download the CA certificate from FortiSASE prior to manually installing it on your endpoints.

To download the FortiSASE CA certificate:

1. Go to *Configuration* > *Security* and select the *Profile Group* using the dropdown list at the top-right.
2. In the *Profiles* tab click *Configure SSL*.
3. Ensure *Deep inspection* is selected for *Inspection method*.
4. For *CA certificate*, select the certificate from the dropdown list. Typically, the default Fortinet_CA_SSL certificate can be used.
5. Click *Download* next to the dropdown list and save the CA certificate to your local computer. You will use this CA certificate in one of the set of instructions below.

Windows

To install the FortiSASE CA certificate on a Windows 10 device:

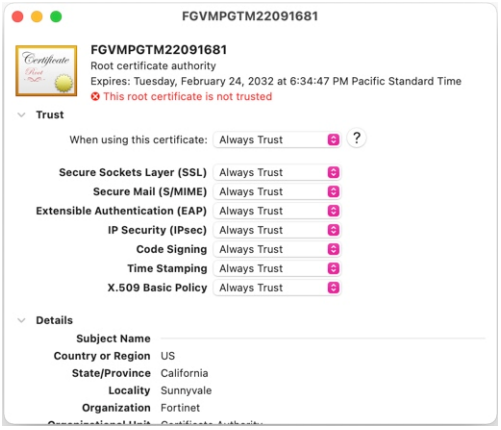
1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. On the *General* tab, click *Install Certificate*.
3. You can install the certificate for the current user or local machine. Installing for the local machine requires administrator permissions. Select the desired option and click *Next*.
4. Choose where you want the certificate to be kept. To customize this, select *Place all certificates in the following store* and browse the store. Then select *Trusted Root Certification Authorities*. Click *Next*.
5. Review and click *Finish* to install the certificate.
6. You can upload and distribute CA certificates using a group policy on multiple Windows devices that are part of an Active Directory. See Distribute certificates to Windows devices by using Group Policy.

macOS

To properly browse any HTTPS websites, you must install the FortiSASE root certificate on the endpoint.

To upload the FortiSASE CA certificate on a mac:

1. Double-click the FortiSASE certificate that the administrator provided during onboarding.
2. From the *Keychain* dropdown list, select *System*, then click *Add*.
3. When you view the certificate, the root certificate appears as not trusted. Expand the *Trust* section. From the *When using this certificate* dropdown list, select *Always Trust*.

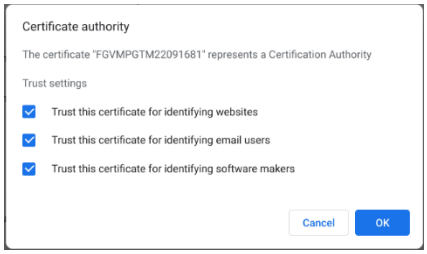


4. Save the configuration and add the certificate to the system keychain. You can connect to HTTPS websites without seeing a warning.

Chrome OS

To upload the FortiSASE CA certificate on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced* > *Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.
5. Click *Import* to import the FortiSASE certificate authority (CA) certificate.
6. If the Fortinet_CA_SSL.cer file does not appear, change the file selection page to show all files. Then select the Fortinet_CA_SSL.cer cert and click open.
7. The next screen asks for your trust settings for this certificate. Select all options, then click *OK*.



8. You have now imported the FortiSASE CA certificate. Scroll down to see the org-Fortinet entry. Expand to see the certificate and view its details.

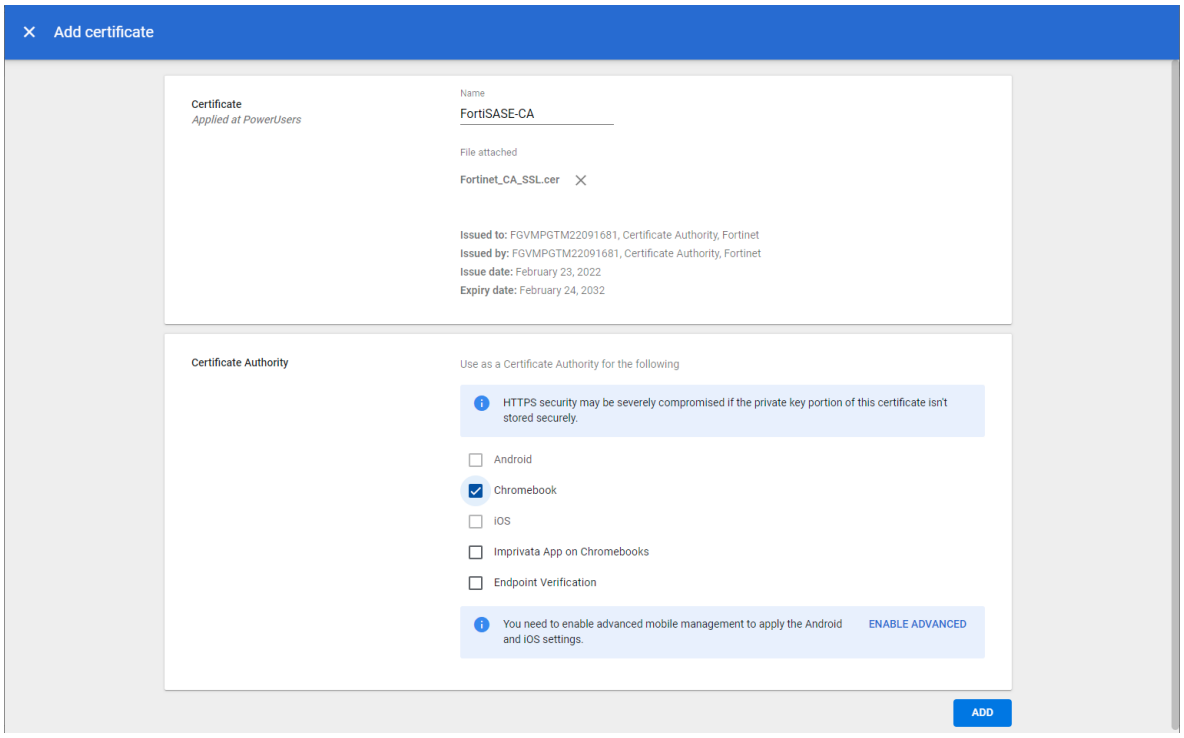
Managed Chromebook

If your organization manages Chromebooks using the Google Admin console, you can centrally install the FortiSASE certificate authority certificate on the Admin console and distribute it to each managed Chromebook.

To upload the FortiSASE CA certificate on Google Admin Console:

1. On the Google Admin console, go to *Device* > *Networks*.
2. Select the organizational unit in which to apply these settings.
3. Under *Certificates*, click *Create Certificate*.
4. Enter a name for this certificate entry, then click *Upload* to upload the Fortinet_CA_SSL.cer certificate.

5. Under *Certificate Authority*, select *Chromebook*. Click *ADD*.



To verify the CA certificate is installed on a Chromebook:

1. In Chrome, open *Settings* from the menu or go to `chrome://settings`.
2. Go to *Privacy and security*. On the configuration page, click *Security*.
3. In the *Security settings* page, scroll to the bottom to find *Advanced* > *Manage certificates*. Click the right arrow.
4. In the *Manage certificate* page, select *Authorities*.
5. Scroll down to the org-Fortinet entry. Expand this entry. You will see the certificate and an icon indicating that Google Admin console is managing it.

Configuring common options for invalid certificates

You can allow or block the passing of traffic with invalid SSL certificates by configuring common options for invalid certificates. For example, when publicly available web sites have expired certificates but users still need to access them, then the allow and keep untrusted action for expired certificates is the desired configuration.

You can configure these options when you configure certificate or deep inspection:

Option	Action to take when...	Default action
Expired certificates	Server certificate is expired.	Block
Revoked certificates	Server certificate is revoked.	
Validation timed-out certificates	Server certificate validation times out.	Allow and keep untrusted
Validation failed certificates	Server certificate validation fails.	Block

The aforementioned options have the following actions:

Action	Description
Allow	Allow the server certificate and keep it untrusted.
Block	Block the certificate.

To configure common options for invalid certificates:

1. Go to *Configuration* > *Security*.
2. At the top of the security profile group page, in the *SSL Inspection* section, click *Customize*.
3. Enable *Certificate Inspection* or *Deep Inspection* as desired.
4. Configure each common option as this topic describes, as desired.
5. Click *OK*.

Blocking QUIC

To ensure security features requiring SSL deep inspection work with HTTP3 traffic, you can manually block QUIC (UDP 443) traffic to ensure fallback from QUIC to TLS 1.3 occurs.

For VPN remote users, you can block QUIC traffic by creating a new policy that blocks QUIC using the predefined QUIC service in FortiSASE.

For secure web gateway (SWG) users, on the endpoint, you can block QUIC traffic by disabling the corresponding web browser setting.

To block QUIC for VPN remote users using a service and policy:

1. Create a policy using the predefined QUIC service by going to *Configuration* > *Policies*:
   a. Click *+Create*.
   b. In the *New Policy* page, configure these settings:

Field	Value
Name	*Block QUIC*
Source Scope	*All*
Destination	*All Internet Traffic*
Service	Click +. Select *QUIC* under *Web Access*. Click *Close*.
Action	*Deny*
Status	*Enable*
Log Violation Traffic	*Enable*

   c. Click *OK*.
2. Drag the newly created policy to the top of the policy list.

To block QUIC for SWG users in web browser settings:

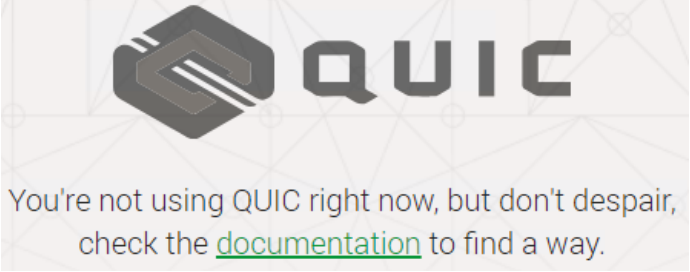
On the endpoint machine, go to the web browser settings and disable QUIC as follows:

Browser	Action
Google Chrome	In the address bar, enter *chrome://flags#enable-quic*, and set *Experimental QUIC protocol* to *Disabled*.
Mozilla Firefox	In the address bar, enter *about:config*, search for *network.http.http3.enabled* and set it to *false*.
Microsoft Edge	In the address bar, enter *edge://flags/#enable-quic*, and set *experimental QUIC protocol* to *Disabled*.

To confirm QUIC has been blocked:

After you have implemented one of the aforementioned approaches to block QUIC traffic, confirm it works as follows:

1. On an endpoint machine, open a web browser. For this example, Google Chrome is used.
2. Go to https://quic.nginx.org/. If QUIC traffic is blocked, you should see the following web site result:



AntiVirus

An AntiVirus (AV) profile allows you to configure FortiSASE to apply AV protection to traffic matching the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- CIFS

AV inspection prevents potentially unwanted and malicious files from entering the network.

Deep inspection is required for AV to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 146.

To apply AV protection to traffic matching certain protocols:

1. Go to *Configuration* > *Security*.
2. In the *AntiVirus* widget, click *Customize*.
3. Under *Inspected Protocols*, enable the toggle for the desired protocol.
4. Click *OK*.

Intrusion prevention

Intrusion Prevention System (IPS) technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

FortiSASE uses signature-based defense against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access, and this communication includes commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing FortiSASE to detect and stop the attack.

Intrusion prevention features are not guaranteed to work when other security features are disabled. It is recommended to enable one of these security features: Antivirus, File filter, DLP, Web filter, or DNS filter.

The following table describes the IPS profiles that you can select in FortiSASE:

	Recommended	Critical	Monitor
Protect client or server traffic	All (client and server)	All (client and server)	All (client and server)
Severity of the signatures	All severity levels: • Info • Low • Medium • High • Critical	• Low • Medium • High • Critical	All severity levels: • Info • Low • Medium • High • Critical
Protocols to be protected	All	All	All
Operating systems to be protected	All: • Windows • Linux • BSD • Solaris • macOS	All: • Windows • Linux • BSD • Solaris • macOS	All: • Windows • Linux • BSD • Solaris • macOS
Applications to be protected	All	All	All

	Recommended	Critical	Monitor
Action taken with traffic in which signatures are detected	Pass or drop matching traffic, depending on the signature default action, which FortiGuard IPS determines	• For signatures with medium, high, and critical severity: block or drop matching traffic. • For signatures with low severity: pass or drop matching traffic, depending on the signature default action, which FortiGuard IPS determines	Monitor, namely, pass or allow matching traffic while logging (monitoring) it.
Enable/disable logging of signatures included in filter	Enable	Enable	Enable

FortiSASE uses the IPS extended database for protection.

For a comprehensive list of protocols and applications protected by FortiGuard IPS signatures that FortiSASE uses, see the IPS database searchable by CVE lookup, ID lookup, or other keywords at Intrusion Prevention Service.

You can also configure custom IPS rules that use custom IPS signatures. To create custom IPS signatures using appropriate signature syntax, see Creating IPS and application control signatures.

To select an IPS profile and configure custom IPS rules to apply to traffic:

1. Go to *Configuration* > *Security* and switch to the *Profiles* tab from the toolbar.
2. In the *Intrusion Prevention* widget, click *Customize*.
3. Select a profile to apply to the traffic:

Profile	Description
Recommended (default)	Scans traffic for all known threats and applies the recommended action.
Critical	Scans traffic for critical threats and blocks them.
Monitor	Scans traffic for threats but does not apply any action. Primarily used for logging.

4. Create custom IPS rules:
   a. In the *Custom IPS rules* section, click *Create*.
   b. In the slide-in, click + on *Signatures*.
   c. In the *Select Entries* slide-in, click + to create custom IPS signature and specify *Tag*, (optional) *Comments*, and *Signature* using the IPS syntax guide. See Creating IPS and application control signatures.
   d. Click *OK*.
5. Click *OK* on the *Confirm* prompt to select the newly created entry.
6. Specify the desired *Action* of *Allow*, *Monitor*, or *Block* for the signature.
7. Click *OK*. The signature created is visible with the desired action inside the *Custom IPS rules* section.

8. Click *OK*.
9. (Optional) Create custom IPS signatures from the *Profile resources* tab.

The custom IPS rules are evaluated first before the configured IPS profile (i.e. recommended, critical, and monitor).

You can use custom IPS rules to manage false positives by configuring a custom IPS signature with *Action* set to *Allow* or *Monitor* and using it in the rule.

To create, edit, and delete a custom IPS signature:

1. Go to *Configuration* > *Security*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.
4. Do one of the following:
   - To create an IPS signature, click *Create*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Intrusion Prevention* widget across different security profiles.
   - To edit an IPS signature, select the desired IPS signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired IPS signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

File Filter

File Filter allows you to block or monitor specific file types. Inspection is based on file type only, not on file content.

Deep inspection is required for File Filter to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 146.

To block traffic by file type:

1. Go to *Configuration* > *Security*.
2. In the *File Filter* widget, click *Customize*.
3. Click into the *Blocked* field.
4. In the *Select Entries* pane, select the desired file types to block.
5. Click *OK*.

DLP

FortiSASE data loss prevention (DLP) prevents sensitive data from leaving or entering your network by defining various sensitive data patterns, scanning for the patterns while inspecting traffic, and allowing, blocking, or logging only when traffic matches the patterns.

DLP rules specify how to handle traffic when a sensor or a file type is triggered. Sensors detect specific content types defined in dictionaries.

DLP is configured based on the following components:

Component	Description
Data type	Define the type of pattern within data or content that DLP tries to match. Currently, DLP supports predefined types such as keyword, regular expressions, hex, credit card, and US social security number.
Data source type	Define the type of data source that DLP tries to match. Currently, DLP supports predefined types such as sensors, MPIP label, or none. With none, DLP matches using only file or message type and protocol as criteria.
Dictionary	Data type entry collections. When selecting a data type such as keyword, regular expressions, or hex, define the pattern that you are looking for.
Sensor	Define which dictionaries to check. You can match any dictionary or all dictionaries., or a special logical combination of the dictionaries. It can also count the number of dictionary matches to trigger the sensor.
File pattern	Define file pattern groups based on predefined file types or define your own pattern to match the file name.
Rule	Define rules for matching a sensor based on a file type or a message, and the protocol type being used. It also allows you to choose the action to allow, block, or log only.

DLP requires deep inspection to decrypt and inspect content in encrypted traffic. See Certificate and deep inspection modes on page 146.

To create a DLP rule:

1. Go to *Configuration* > *Security*.
2. For *Profile Group*, select an existing profile group to edit or create a new profile group using + in the *Profile Group* dropdown list.
3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the *SSL Inspection* widget, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Customize*.
   b. Select *Deep Inspection*.
   c. Click *OK*.
5. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.

b. In the DLP slide-in, click *Create* to create a new DLP rule.

c. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	Rule name.
Data Source Type	Select the type of data source that DLP tries to match. When you select *Sensors* or *MPIP Label*, you must select or create a new DLP sensor or sensitivity label, respectively.
Sensor	If you select *Sensors* for *Data Source Type*, select DLP sensors. You must create a new DLP sensor and then select it.
Sensitivity Label	If you select *MPIP Label* for *Data Source Type*, then select a sensitivity label. You must create a new sensitivity label and then select it.
Severity	Select the severity or threat level that matches this filter.
Action	Action to take with content that this DLP profile matches.
Type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).
File type	Select the number of a DLP file pattern table to match. You can either select a predefined file pattern table or create a new one by clicking + in the dropdown list.
Protocol	Check messages or files over one or more of these protocols.

6. Do one of the following:

a. If you selected *Sensors* for *Data Source Type*, do the following:

i. Create a new sensor by clicking + next to *Sensor*. In the *Select Entries* slide-in, click + *Create* to the right to create a new sensor. In the *New Sensor* slide-in, configure these settings:

Field	Description
Name	Sensor name.
Entry matches needed to trigger sensor	Logic used to apply to sensor entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of entries	Create one or more entries.

ii. Create a sensor entry by clicking +*Create*. In the *New Entry* slide-in, configure these settings:

Field	Description
ID	Numerical ID for the sensor entry
Dictionary	Select the dictionary for this sensor entry. You must create a new dictionary and then select it.
Dictionary matches needed to consider traffic DLP risk	Number of dictionary matches to trigger sensor entry.
Status	Select whether the sensor entry is Enabled or Disabled.

iii. Create a dictionary by clicking the *Dictionary* field and click *+Create* to create a new DLP dictionary. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Description
Name	Dictionary name.
Entry matches needed to trigger sensor	Logic used to apply to dictionary entry matches to trigger sensor: • *All*: logical AND condition on matching entries • *Any*: logical OR condition on matching entries
Table of Dictionary Entries	Create one or more dictionary entries.

iv. Create a new dictionary entry by clicking *+Create*. In the *New Entry* slide-in, configure these settings:

Field	Description
Type	Select a predefined *DLP Data Type* from the dropdown list.
Repeat	Enable or disable repeat matching of the selected *DLP Data Type*.
Status	Select whether the dictionary entry is *Enabled* or *Disabled*.

v. Click *OK* to create the new dictionary entry.
vi. Click *OK* to create the DLP dictionary. You will be prompted to select the newly created dictionary.
vii. Click *OK* to create the new sensor entry.
viii. Click *OK* to create the new sensor. You will be prompted to select the newly created sensor.
ix. Click *OK* to create the new DLP rule.

b. If you selected *MPIP Label* for *Data Source Type*, do the following:
i. Create a sensitivity label by clicking + next to *Sensitivity Label*.
ii. In the *Create MPIP sensitivity label* slide-in, configure these settings:

Field	Description
Name	Sensitivity label name.
Sensitivity level GUID	Enter the globally unique identifier (GUID) for your sensitivity label. See Learn about sensitivity labels.

iii. Click *OK*.
iv. Click *OK* to create the sensitivity label. FortiSASE prompts you to select the newly created sensitivity label.
v. Click *OK* to create the new DLP rule.

7. Click and drag the DLP rules in the desired order.

Repeat any aforementioned step to create multiple entries for these settings:
- Dictionary entries
- DLP dictionaries
- Sensor entries
- Sensors
- DLP rules

8. Configure the updated profile group in a policy:
   a. Go to *Configuration* > *Policies*.
   b. Select an existing policy to apply the profile group to and click *Edit*. Alternatively, create a new policy to apply the profile group to.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select the desired profile group. The *Profile Group* field is only available for policies where *Action* is configured as *Accept*.
   d. Click *OK*.

Blocking HTTPS upload traffic with credit card info example

This configuration will block HTTPS upload traffic that includes credit card information. The pre-defined data type for credit card is used in the dictionary.

To configure blocking HTTPS upload traffic that includes credit card information:

1. Go to *Configuration* > *Security*.
2. For *Profile Group*, create a new profile group using + in the *Profile Group* dropdown list.
   a. In the *Create Profile Group* slide-in configure these settings:
      i. In the *Name* field, enter Custom-DLP-1.
      ii. For *Initial Configuration*, select *Basic*.
   b. Click *OK*.
   c. When prompted to select the new entry, click *OK*.
3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter, Application Control With Inline-CASB) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the SSL Inspection widget ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Customize*:
   b. Select *Deep Inspection*.
   c. Click *OK*.
5. Enable *Data Loss Prevention (DLP)*.
6. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click *Customize*.
   b. In the DLP slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Value
Name	dlp-case-1
Sensors	Select DLP sensors. You must create a new DLP sensor and then select it.
Severity	*Medium*
Action	*Block*
Type	*File*
File type	*builtin-patterns*

Field	Value
Protocol	*HTTP-GET, HTTP-POST*

d. Create a new sensor:
  i. Create a new sensor by clicking + next to *Sensor*.
  ii. In the *Select Entries* slide-in, click *+ Create* to the right to create a new sensor.
  iii. In the *New Sensor* slide-in, configure these settings:

Field	Value
Name	sensor-case-1
Entry matches needed to trigger sensor	*Any*
Table of entries	Create a new entry.

e. Create a sensor entry:
  i. Create a new sensor entry by clicking *+Create*.
  ii. In the *New Entry* slide-in, configure these settings:

Field	Value
ID	*1*
Dictionary	Select the dictionary for this sensor entry. You must create a new dictionary and then select it.
Dictionary matches needed to consider traffic DLP risk	*1*
Status	*Enabled*

f. Create a dictionary:
  i. Click the *Dictionary* field and click *+Create* to create a new DLP dictionary.
  ii. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Value
Name	dl-case-1
Entry matches needed to trigger sensor	*Any*
Table of Dictionary Entries	Create one or more dictionary entries.

g. Create a dictionary entry:
  i. Create a new dictionary entry by clicking *+Create*.
  ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	credit-card

Field	Value
Repeat	*Disable*
Status	*Enabled*

h. Click *OK* several times to complete the customization:
   i. Click *OK* to create the new dictionary entry.
   ii. Click *OK* to create the DLP dictionary. Click *OK* when prompted to select the newly created dictionary.
   iii. Click *OK* to create the new sensor entry.
   iv. Click *OK* to create the new sensor. Click *OK* when prompted to select the newly created sensor. Click *Close*.
   v. Click *OK* to create the new DLP rule.
   vi. Click *OK* to complete DLP configuration customization.

7. Configure the updated profile group in a policy:
   a. Go to *Configuration* > *Policies*.
   b. Configure a new policy with these settings:

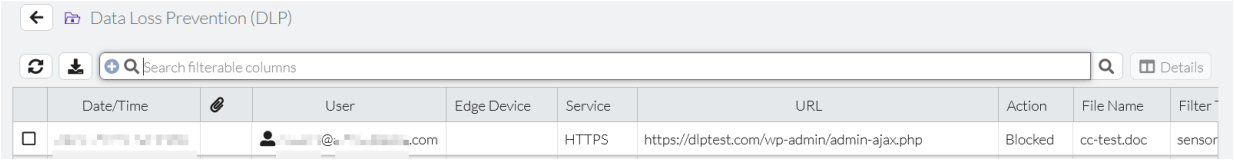
Field	Value
Name	Test-DLP-1
Source Scope	*VPN Users*
Source	*All Traffic*
User	*All VPN Users*
Destination	*All Internet Traffic*
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *Custom-DLP-1*
Status	*Enable*
Log Allowed Traffic	*Enable* Select *All Sessions*

   c. Click *OK*.
8. Drag the *Test-DLP-1* to the top of the policy list. Ensure it is placed above *Allow-All*.

To verify blocking HTTPS upload traffic that includes credit card information is working:

1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://dlptest.com/sample-data/. Copy one of the credit card numbers from the page and paste it into a Word document. Save the document in .DOC format to your endpoint local drive as cc-test.doc.

4. Go to https://dlptest.com/https-post/. Under *File Upload*, select the .DOC file created and click *Submit*. Since HTTP POST traffic for the PDF file upload includes a credit card number, FortiSASE blocks the file and generates a DLP log.
5. In FortiSASE, go to *Analytics* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your VPN user and cc-test.doc filename.



Blocking ChatGPT using keywords and FQDN example

Large language models (LLMs), such as GPT, which are a type of Generative AI (GenAI), are widely used in applications like chatbots.

This configuration blocks HTTPS upload traffic to the OpenAI ChatGPT application that includes a sensitive keyword. The predefined data type, keyword, is used in the DLP dictionary.

This example configures blocking QUIC so that the OpenAI server uses TLS 1.3 instead of QUIC. FortiSASE can inspect TLS 1.3 traffic using SSL deep inspection.

To configure blocking HTTPS upload traffic that includes sensitive keywords:

1. Go to *Configuration* > *Security*.
2. For *Profile Group*, create a new profile group using + in the *Profile Group* dropdown list.
   a. In the *Create Profile Group* slide-in configure these settings:
      i. In the *Name* field, enter ChatGPT.
      ii. For *Initial Configuration*, select *Basic*.
   b. Click *OK*.
   c. When prompted to select the new entry, click *OK*.
3. Disable AntiVirus, Web Filter with Inline-CASB, and DNS Filter using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. Observe that SSL inspection should already be enabled and is set to *Certificate Inspection*. Click *Configure SSL* and configure *Deep Inspection* using Fortinet_CA_SSL as the CA certificate accordingly.
5. Create a policy using the predefined QUIC service by going to *Configuration* > *Policies*:
   a. Click *+Create*.
   b. In the *New Policy* page, configure the following:

Field	Value
Name	Block QUIC
Source Scope	*All*
Destination	*All Internet Traffic*

Field	Value
Service	Click +. Select *QUIC* under *Web Access*. Click *Close*.
Action	*Deny*
Status	*Enable*
Log Violation Traffic	*Enable*

c. Click *OK*.
d. Drag the newly created policy to the top of the policy list.

6. Enable *Data Loss Prevention (DLP)*.
7. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click *Customize*.
   b. In the DLP slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Value
Name	chatgpt
Sensors	Select DLP sensors. You must create a new DLP sensor and then select it.
Severity	*Critical*
Action	*Block*
Type	*Message*
Protocol	*HTTP-POST*

   d. Create a new sensor:
      i. Create a new sensor by clicking + next to *Sensor*.
      ii. In the *Select Entries* slide-in, click + *Create* to the right to create a new sensor.
      iii. In the *New Sensor* slide-in, configure these settings:

Field	Value
Name	chatgpt
Entry matches needed to trigger sensor	*Any*
Table of entries	Create a new entry.

e. Create a sensor entry:

i. Create a new sensor entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
ID	*1*
Dictionary	Select the dictionary for this sensor entry. You must create a new dictionary and then select it.
Dictionary matches needed to consider traffic DLP risk	*1*
Status	*Enabled*

f. Create a dictionary:

i. Click the *Dictionary* field and click *+Create* to create a new DLP dictionary.

ii. In the *New DLP Dictionary* slide-in, configure these settings:

Field	Value
Name	chatgpt
Entry matches needed to trigger sensor	*All*
Table of Dictionary Entries	Create two dictionary entries as follows.

g. Create a dictionary entry with the *programming* keyword by doing the following:

i. Create a new dictionary entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	*keyword*
Pattern	programming
Case sensitive	Enable
Repeat	Disable
Status	Enabled

The configuration enables *Case sensitive* to enable ignoring letter case when pattern matching.

h. Create a dictionary entry with the *tips* keyword by doing the following:

i. Create a new dictionary entry by clicking *+Create*.

ii. In the *New Entry* slide-in, configure these settings:

Field	Value
Type	*keyword*
Pattern	tips

Field	Value
Case sensitive	Enable
Repeat	Disable
Status	Enabled

The configuration enables *Case sensitive* to enable ignoring letter case when pattern matching.

i. Click *OK* several times to complete the customization:
   i. Click *OK* to create the new dictionary entry.
   ii. Click *OK* to create the DLP dictionary. Click *OK* when prompted to select the newly created dictionary.
   iii. Click *OK* to create the new sensor entry.
   iv. Click *OK* to create the new sensor. Click *OK* when prompted to select the newly created sensor. Click *Close*.
   v. Click *OK* to create the new DLP rule.
   vi. Click *OK* to complete DLP configuration customization.

8. Configure the updated profile group in a policy:
   a. Go to *Configuration* > *Policies*.
   b. Configure a new policy with these settings:

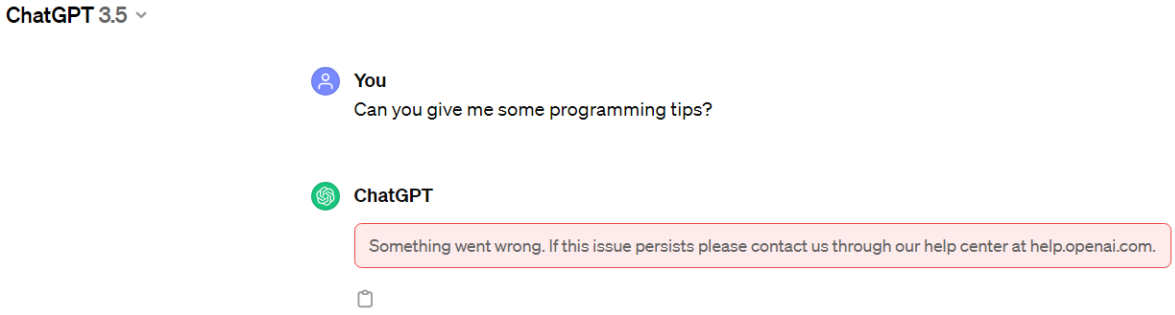
Field	Value
Name	ChatGPT
Source Scope	*All*
Destination	*Specify:* 1. Click +. 2. In the *Select Entries* slide-in, click + and create new + *IPv4 Host*. 3. In the *New Host* slide-in, configure these settings: a. *Location*: *Unspecified* b. *Name*: ChatGPT c. *Type*: *FQDN* d. *FQDN*: chatgpt.com 4. Click *OK* to create the new host. 5. Click *OK* when prompted to select the newly created host. 6. Click *Close*.
Service	*ALL*
Action	*Accept*
Profile Group	*Specify* Select *ChatGPT*
Status	*Enable*
Log Allowed Traffic	*Enable* Select *All Sessions*

   c. Click *OK*.

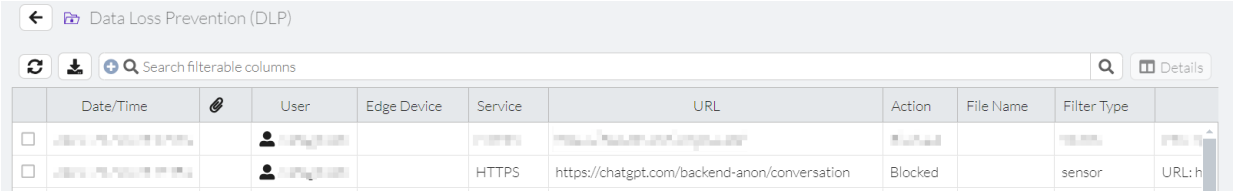
9. Drag the *ChatGPT* policy to the top of the policy list. Ensure it is placed above *Allow-All*.

To verify blocking HTTPS upload traffic that includes sensitive keywords is working:

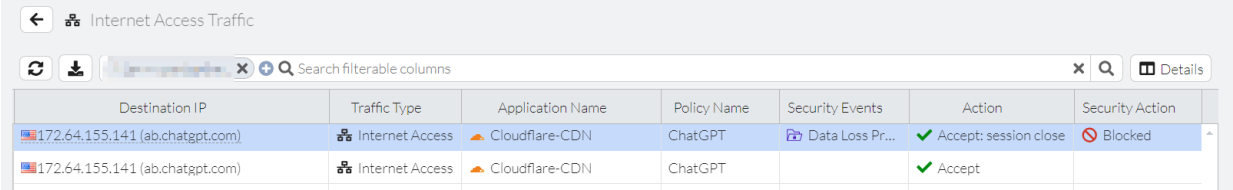
1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://chatgpt.com.
4. Search for any phrase that includes the keywords set up in the DLP dictionary. Since the phrase in HTTP POST traffic includes both sensitive keywords, FortiSASE blocks this traffic to ChatGPT and generates a DLP log. Verify the request fails in ChatGPT and an error is generated.



5. In FortiSASE, go to *Analytics* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your VPN user and visiting https://chatgpt.com.



6. Go to *Analytics* > *Security* > *Traffic* > *Internet Access Traffic* and confirm that FortiSASE generated a DLP block log entry that corresponds to your VPN user and visiting https://chatgpt.com.



Blocking file with MPIP sensitivity label example

To safeguard your organization's data, you can employ labels as markers for sensitive information. Microsoft provides sensitivity labels, which act as identifiers emphasizing the importance of the data that they are associated with, thereby enhancing the security measures in place. See Protect your sensitive data with Microsoft Purview.

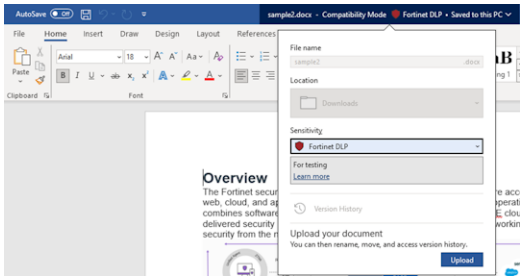
You can effectively manage any data traffic that includes a sensitivity label using FortiSASE. Usage of a predefined data source type, MPIP Label, specifically designed for matching MPIP sensitivity labels previously applied to files, makes this possible.

This configuration blocks HTTPS upload traffic that includes an MPIP sensitivity label.

To complete prerequisites:

Before configuring FortiSASE, complete the following steps:

1. Create and configure sensitivity labels and their policies. See Create sensitivity labels.
2. Apply a sensitivity label to content. See Apply sensitivity labels to your files and email. Once the sensitivity label is applied on a file, it displays on the sensitivity bar.



3. Obtain the globally unique identifier (GUID) for your sensitivity labels. See Search for documents by sensitivity label. The following shows a sample GUID:

```
PS C:\Windows\system32> Get-Label |Ft Name, Guid

Name                                Guid
----                                ----
Fortinet DLP                        ca51e4ff-0733-4744-bebb-d3e1eb6383f4
```

FortiSASE uses the GUID for label matching. The value of *Sensitivity level GUID* is configured to correspond to the label's GUID.

To configure blocking HTTPS upload traffic that includes an MPIP sensitivity label applied:

1. Go to *Configuration* > *Security*.
2. For *Profile Group*, select an existing profile group to edit or create a new profile group using + in the *Profile Group* dropdown list.
3. Disable all enabled security features (AntiVirus, Web Filter with Inline-CASB, Intrusion Prevention, DNS Filter) using these steps for each security feature:
   a. Click the toggle button next to the security feature widget to disable the feature.
   b. Click *OK* to confirm disabling the security feature.
4. In the *SSL Inspection* widget, ensure deep inspection is enabled:
   a. For *SSL inspection*, click *Customize*.
   b. Select *Deep Inspection*.
   c. Click *OK*.
5. Create a DLP rule:
   a. In the *Data Loss Prevention (DLP)* widget, click the toggle button to enable this feature, and then click *Customize*.
   b. In the *DLP* slide-in, click *Create* to create a new DLP rule.
   c. In the *New Rule* slide-in, configure these settings:

Field	Description
Name	Rule name.

Field	Description
Data Source Type	Select *MPIP Label*. You must select or create a new sensitivity label.
Sensitivity Label	Create a new sensitivity label and then select it.
Severity	Select the severity or threat level that matches this filter.
Action	Action to take with content that this DLP profile matches.
Type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).
File type	Select the number of a DLP file pattern table to match. You can either select a predefined file pattern table or create a new one by clicking + in the dropdown list.
Protocol	Check messages or files over one or more of these protocols.

6. Create a new sensitivity label:
   a. Create a new sensitivity label by clicking + next to *Sensitivity Label*.
   b. In the *Create MPIP sensitivity label* slide-in, configure these settings:

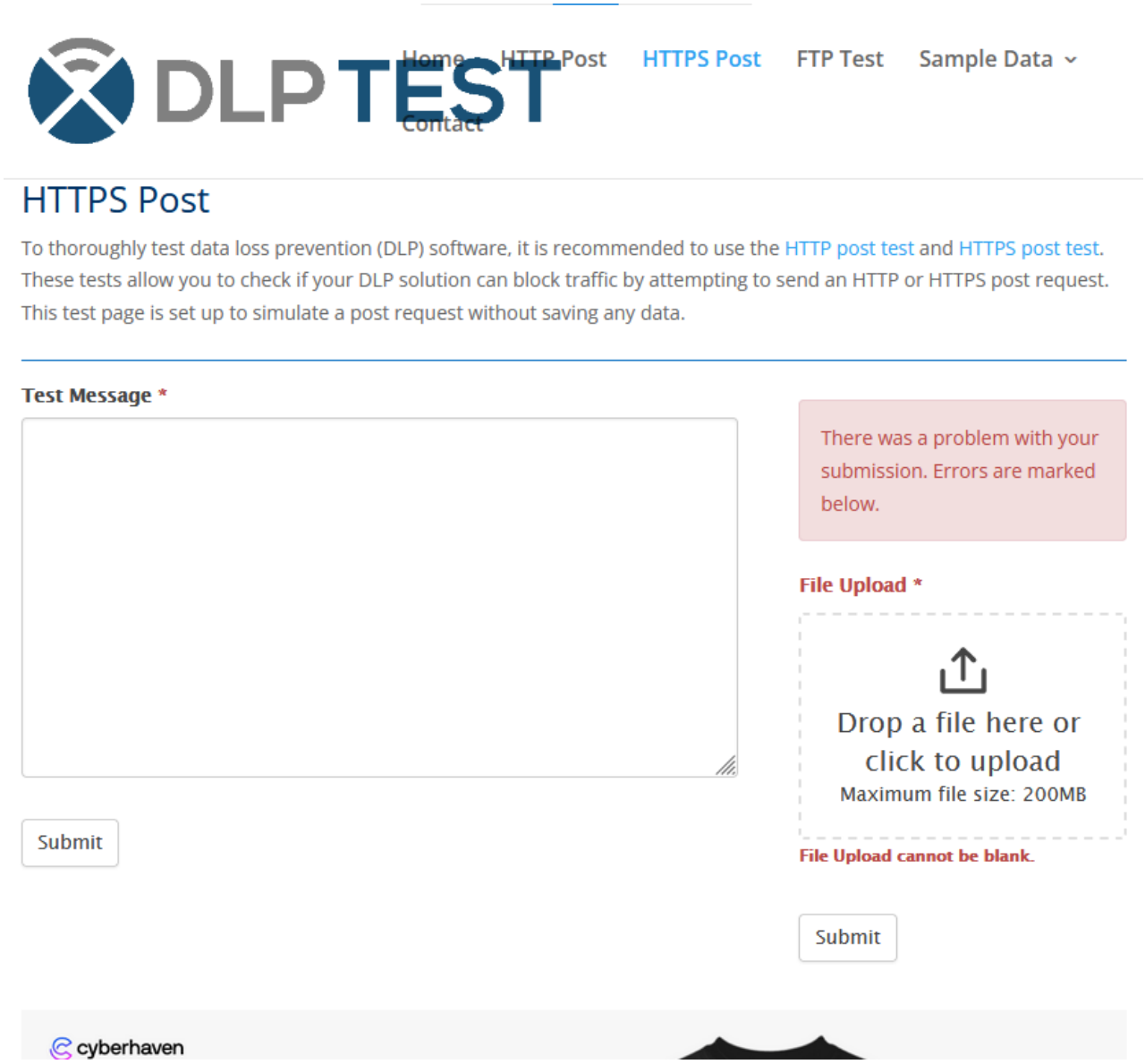
Field	Description
Name	Sensitivity label name.
Sensitivity level GUID	Enter the globally unique identifier (GUID) for your sensitivity label. See To complete prerequisites: on page 168 for how to obtain the GUID for your sensitivity label.

   c. Click *OK*.
7. Click *OK* twice to complete creating the DLP rule:
   a. Click *OK* to create the sensitivity label. You will be prompted to select the newly created sensitivity label.
   b. Click *OK* to create the new DLP rule.
8. Configure the updated profile group in a policy:
   a. Go to *Configuration* > *Policies*.
   b. Select an existing policy to apply the profile group to and click *Edit*. Alternatively, create a new policy to apply the profile group to.
   c. In the *Profile Group* field, select *Specify*. From the dropdown list, select the desired profile group. The *Profile Group* field is only available for policies where *Action* is configured as *Accept*.
   d. Click *OK*.

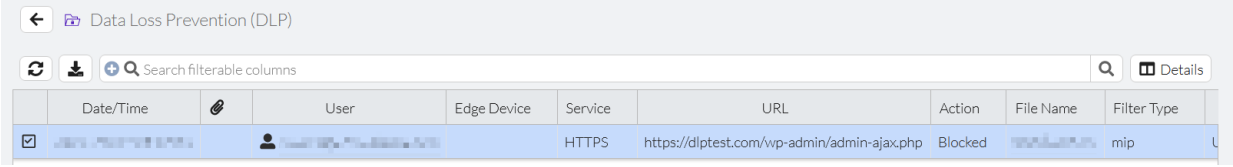
To configure blocking HTTPS upload traffic that includes an MPIP sensitivity label applied is working:

1. Ensure that your endpoint with FortiClient installed is registered with FortiSASE Endpoint Management Service and that you have established a secure connection to FortiSASE.
2. On the connected endpoint, open the Chrome web browser in incognito mode.
3. In the web browser, go to https://dlptest.com/https-post/
4. Upload a Word document file with an MPIP sensitivity label applied.

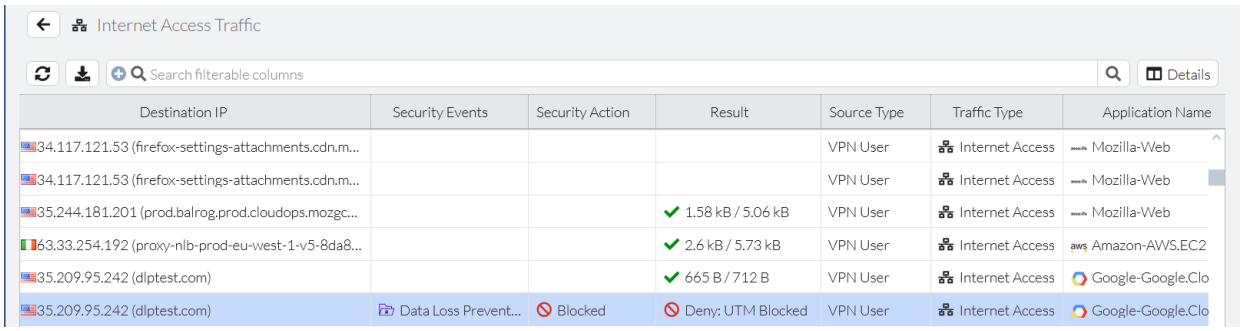
5. Observe that the file upload fails before and after file submission:



6. In FortiSASE, go to *Analytics* > *Security* > *Data Loss Prevention (DLP)* and confirm that FortiSASE generated a DLP block log entry that corresponds to your VPN user and visiting https://dlptest.com/https-post/



7. Go to *Analytics* > *Security* > *Traffic* > *Internet Access Traffic* and confirm that FortiSASE generated a DLP block log entry that corresponds to your VPN user and visiting https://dlptest.com/https-post/



Web Filter

Web filter restricts or controls user access to web resources. In FortiSASE, there are three main components of Web Filter:

Component	Description
URL Category	Provides categories from the FortiGuard Web Filter service that you can use to filter web traffic.
URL Filter	Uses specific URLs with patterns containing text and regular expressions so FortiSASE can process the traffic based on the filter action (exempt, block, allow, monitor) and webpages that match the criteria.
Content Filter	Blocks or exempts webpages containing words or patterns that you specify. Additionally, in HTTPS connections, since the HTTP payload is encrypted, the default certificate inspection cannot inspect the traffic. To apply content filter on HTTPS traffic, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

These components interact with each other to provide maximum control over what users on your network can view and protect your network from many internet content threats.

FortiSASE applies web filters in the following order:

1. URL Filter
2. URL Category
3. Content Filter

In FortiSASE, by default, there is one global Web Filter configuration that applies to all users using a default security profile group applied to a default allow VPN or SWG policy. Administrators can customize configuration for Web Filter and other security features by creating a custom security profile group, customizing settings for the new profile group, creating a new VPN or SWG policy with selected users or user groups specified, and then applying the profile group to the policy.

FortiSASE supports these Web Filter options:

Option	Description
Block Invalid URLs	Block websites when their SSL certificate CN field does not contain a valid domain name.

Option	Description
	This option also blocks URLs that contains spaces. If there is a space in the URL, you must write it as %20 in the URL path.
Allow websites when a rating error occurs	Allow access to websites that return a rating error from the FortiGuard Web Filter service.
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	This setting applies to popular search sites and prevents explicit websites and images from appearing in search results. The supported search sites are Google, Yahoo, Bing, and Yandex. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

Restricting web usage using FortiGuard URL categories and URL filter

To restrict web usage using FortiGuard URL categories and URL filter:

1. Go to *Configuration* > *Security*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. Enable *FortiGuard Category Based Filter*.
4. By default, FortiSASE allows access to FortiGuard categories when you enable the FortiGuard category-based filter. To change the category action to *Monitor* or *Block*, select the desired category, then select *Monitor* or *Block*. The following provides descriptions of the actions:

Type	Description
Allow	Passes the traffic to the remaining web filters, antivirus inspection engine, and DLP inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies or blocks attempts to access any URL that belongs to the category. A replacement message displays.

5. Under *URL Filter*, click *Create*.
6. Configure the URL filter:
   a. In the *URL* field, enter the desired URL.
   b. For *Type*, select one of the following:

Type	Description
Simple	Tries to strictly match the full context. For example, if you enter www.facebook.com in the *URL* field, it only matches traffic with www.facebook.com. It does not match facebook.com or message.facebook.com. When FortiSASE finds a match, it performs the selected URL action.

Type	Description
Wildcard	Tries to match the pattern based on the rules of wildcards. For example, if you enter *fa* in the *URL* field, it matches all the content that has fa such as www.facebook.com, message.facebook.com, fast.com, and so on. When FortiSASE finds a match, it performs the selected URL action.
RegExp	Tries to match the pattern based on the rules of regular expressions. When FortiSASE finds a match, it performs the selected URL action.

c. For *Action*, select one of the following:

Type	Description
Allow	Passes the traffic to the remaining web filters, antivirus inspection engine, and DLP inspection engine. If the URL does not appear in the URL list, FortiSASE allows the traffic.
Block	Denies or blocks attempts to access any URL that matches the URL pattern. A replacement message displays.
Exempt	Allows the traffic to pass through, bypassing other web filters, antivirus inspection engine, and DLP inspection engine.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.

d. Configure the status as desired.

7. Click *OK*.

Restricting web usage using content filter

Restricting web usage using content filter for HTTPS pages requires enabling SSL deep inspection. See Certificate and deep inspection modes on page 146.

To restrict web usage using content filter:

1. Go to *Configuration* > *Security*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. Under *Content Filter*, click *Create*.
4. For *Pattern Type*, select one of the following:

Type	Description
Wildcard	Blocks or exempts one word or text strings of up to 80 characters. You can also use wildcard symbols such as ? or * to represent one or more characters. For example, a wildcard expression forti*.com matches fortinet.com and fortiguard.com. The * represents any character appearing any number of times.

Type	Description
RegExp	Blocks or exempts patterns of regular expressions that use some of the same symbols as wildcard expressions, but for different purposes. In regular expressions, * represents the character before the symbol. For example, forti*.com matches fortiii.com but not fortinet.com or fortiice.com. In this case, the symbol * represents i appearing any number of times.

5. In the *Pattern* field, enter the desired pattern.
6. From the *Language* dropdown list, select the desired language.
7. For *Action*, select one of the following:

Type	Description
Exempt	Allows the traffic to pass through, bypassing other content filters, antivirus inspection engine, and DLP inspection engine.
Block	Denies or blocks attempts to access any URL that matches the URL pattern. A replacement message displays.

8. Configure the status as desired.
9. Click *OK*.

Web rating override using custom categories

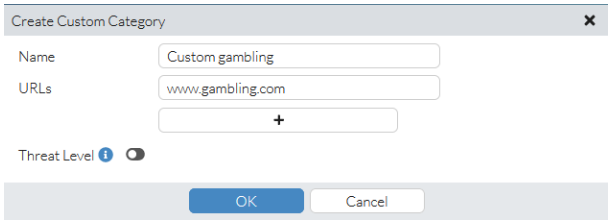
Web rating overrides allow you to add specific URLs to custom web ratings categories.

In a web filter profile, you can configure the action for each category. See Restricting web usage using FortiGuard URL categories and URL filter on page 172 for details. If a URL is in multiple categories, custom categories take precedence over FortiGuard categories.

For example, consider that you add www.gambling.com is added to a custom category and set the custom category action to Block. The default action for the FortiGuard Gambling category is Monitor. When a user browses to www.gambling.com, the custom category action takes precedence over the FortiGuard category, so access to www.gambling.com is blocked.

To configure web rating override using a custom category:

1. Go to *Configuration* > *Security* > *Profile resources* > *Custom Web Filter categories*.
2. Create a custom category:
   a. Click *Create Custom Category*.
   b. In the *URLs* field, enter the desired URL. In this example, it is www.gambling.com.
   c. Configure other fields as desired.
   d. Click *OK*.



3. Go to Profiles.
4. In the *Web Filter With Inline-CASB* widget, click *Customize*.
5. Under *FortiGuard Category Based Filter* > *Custom Categories*, select the newly created category, then select the desired action. In this example, it is *Block*.
6. Click *OK*.

Enforcing safe search in web filter

To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

To enforce safe search in web filter:

1. Go to *Configuration* > *Security*.
2. Create a new profile group by clicking on the dropdown next to *Profile Group* and clicking the plus sign (+) or select an existing profile group.
3. Enable *Web Filter With Inline-CASB*.
4. Under *Web Filter With Inline-CASB*, click *Customize*.
5. Under the *Settings* tab, scroll down to the *Options* section and enable *Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex*.
6. Click *OK*.

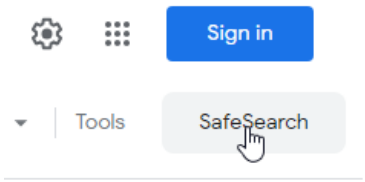
For individual search engine safe search specifications, refer to the documentation for Google, Yahoo, Bing, and Yandex.

To validate safe search after enforcing it in web filter:

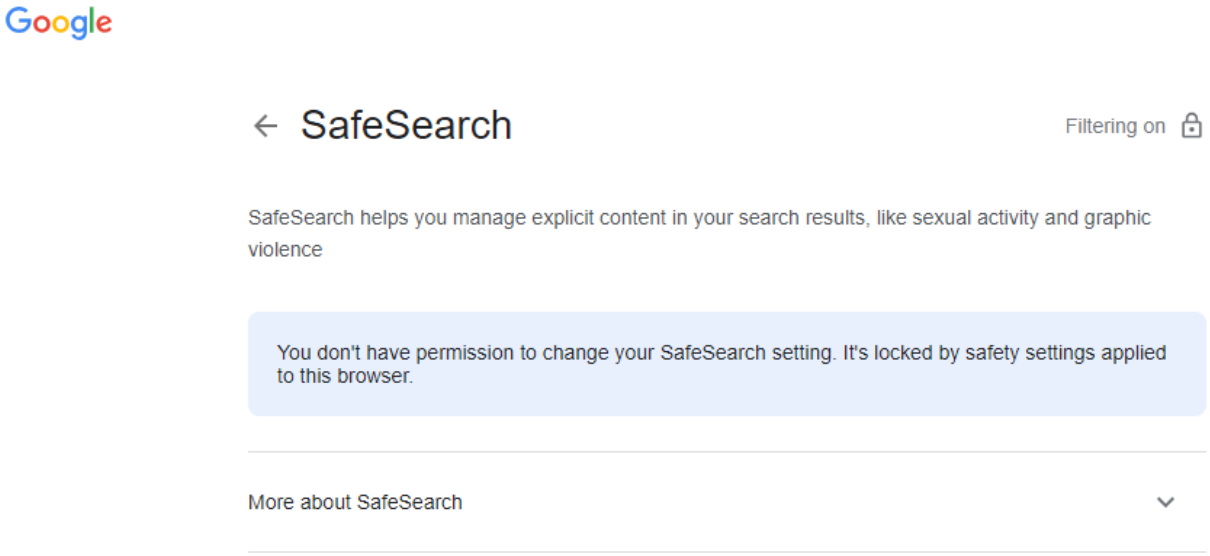
Safe search is still enforced from FortiSASE even if the individual search engine allows you to disable safe search from their search engine interface.

In the examples below, safe search was disabled for each of the individual search engines (except for Google which does not allow any modification).

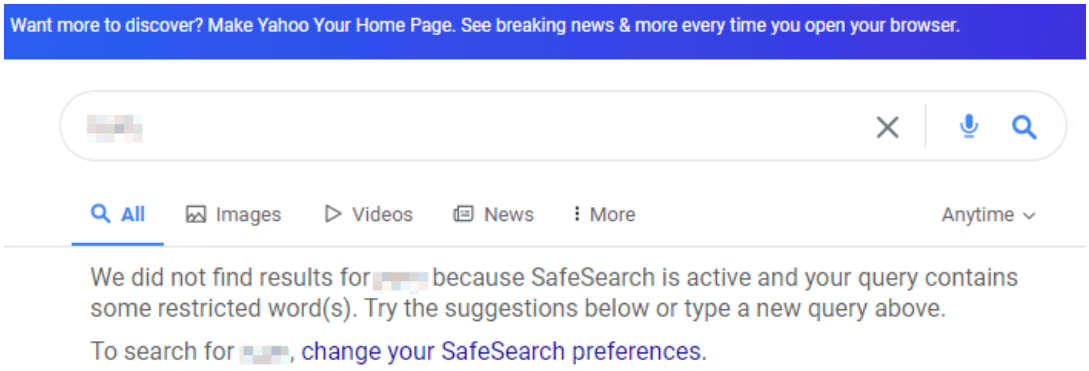
1. Go to a web browser, browse to Google and perform a search:
   a. Observe in the top-right corner that SafeSearch is enabled and cannot be modified.



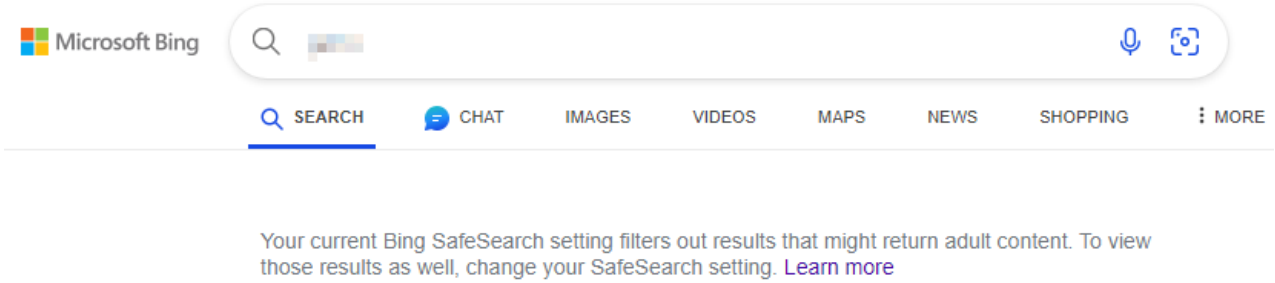
b. If you click on SafeSearch, then you will see the following message:



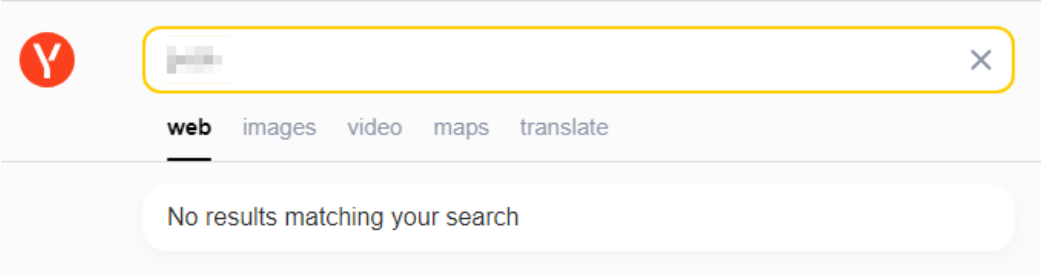
2. Go to a web browser, browse to Yahoo, perform a search, and observe that search results matching safe search criteria are blocked:



3. Go to a web browser, browse to Bing, perform a search, and observe that search results matching safe search criteria are blocked:



4. Go to a web browser, browse to Yandex, perform a search, and observe that search results matching safe search criteria are blocked:



Customizing inline-CASB headers

The FortiSASE Web Filter with Inline-CASB security component can be used to customize headers when agentless (SWG) or agent-based (FortiClient) remote users are accessing SaaS applications. When configured, FortiSASE intercepts HTTP headers and can modify them for outgoing traffic as follows:

- Add to request
- Add to response
- Remove from request
- Remove from response

The process of intercepting and customizing HTTP headers is also commonly known as HTTP header insertion.

By customizing HTTP headers for FortiSASE outgoing traffic destined for SaaS applications, the Web Filter with Inline-CASB can control SaaS application behaviour. Typically, customizing headers, namely, adding to request headers for access requests to SaaS applications is used to implement restricting tenants' access.

Prerequisites

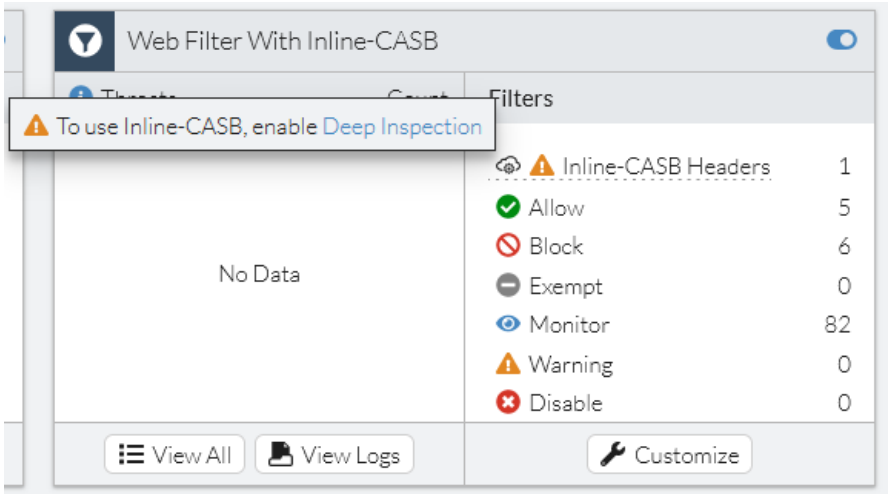
SSL deep inspection

Customizing HTTP headers using the Web Filter with Inline-CASB requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept HTTP headers and add and remove them to header requests and responses as the SaaS application requires.

- To confirm SSL deep inspection is enabled, go to *Configuration* > *Security* and under the *SSL Inspection* widget, ensure that *Deep Inspection* displays.
- To enable SSL deep inspection, go to *Configuration* > *Security* and in the *SSL Inspection* widget, click *Customize*, and in the *SSL Inspection* slide-in, select *Deep Inspection* and click *OK*.

If you do not enable deep inspection, you see the following warnings:

- Under *Configuration* > *Security* in the *Web Filter With Inline-CASB* widget, you see a caution icon and when hovering over the tooltip, you see a warning message with a link to the *Deep Inspection* page.



- When clicking on *Customize* in the *Web Filter With Inline-CASB* widget and selecting the *Inline-CASB Headers* tab, you see a warning message with a link to the *Deep Inspection* page.

See Certificate and deep inspection modes on page 146.

SaaS vendor-specific headers

You must know the format and content of vendor-specific headers supported by a SaaS application to use with the Web Filter with Inline-CASB.

For more information on the specific headers used for restricted SaaS access, see SaaS vendor-specific documentation:

Vendor	Documentation link
Office 365	Restrict access to a tenant
Google Workspace	Block access to consumer accounts
Slack	Approve Slack workspaces for your network

Currently, all configured headers are added to outgoing FortiSASE traffic for agentless (SWG) remote users. Therefore, for this scenario, ensure you configure headers carefully considering their global scope to ensure they do not overlap or result in duplicate behaviour.

Customizing inline-CASB headers for restricted SaaS access

Large organizations may want to restrict SaaS access to resources like Microsoft Office 365, Google Workspace, and Slack by tenants to block non-company login attempts and secure the users from accessing non-approved cloud resources. Many cloud vendors enable this by applying tenant restrictions for access control. For example, users accessing Microsoft 365 applications with tenant restrictions through the corporate proxy are only allowed to log in as the company's tenant and access the organization's applications.

Typically, access requests from clients pass through a security device or service, in this case FortiSASE, which inserts headers to notify the SaaS service to apply tenant restrictions with the permitted tenant list. Users are redirected to the SaaS service login page and can only log in if they belong to the permitted tenant list.

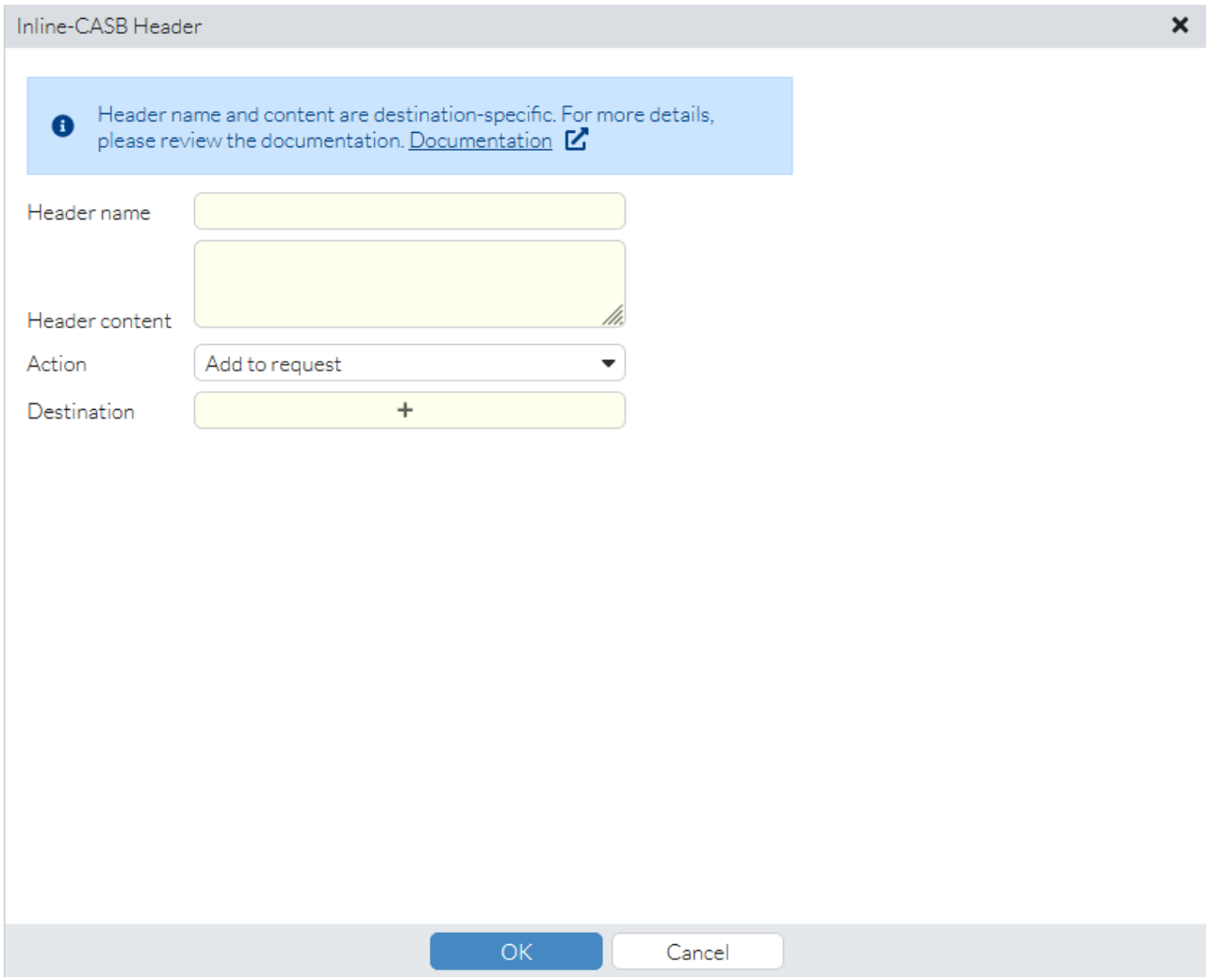
To customize headers for Office 365 tenant restriction, Google Workspace account access control, and Slack-approved workspaces for current network:

Ensure that you have reviewed Prerequisites on page 177 and have them in place before proceeding to customize headers to ensure proper functionality.

1. Go to *Configuration* > *Security* and select the desired *Profile Group*.
2. In the *Web Filter With Inline-CASB* widget, click *Customize*.
3. In the *Web Filter With Inline-CASB* slide-in, click the *Inline-CASB Headers* tab, then click *Create* to create a new inline-CASB header.
4. In the *Inline-CASB Header* slide-in, configure an inline-CASB header according to the vendors' specifications:
   a. Set the *Header name*. The service provider defines this.
   b. Set the *Header content* or HTTP header content to be inserted into the traffic. Your settings define this.
   c. Set the *Action* to one of the following:

Action when HTTP header is forwarded	Description
Add to request (default)	Add the HTTP header to request.
Add to response	Add the HTTP header to response.
Remove from request	Remove the HTTP header from request.
Remove from response	Remove the HTTP header from response.

   d. Set the *Destination*. This is an address object or address group containing domains that the service provider specifies.



5. Click *OK* to save the configured inline-CASB header.
6. Configure the applicable policy to use the security profile group with the Web Filter With Inline-CASB containing the newly configured Inline-CASB header:
   - For FortiClient agent-based remote users, go to *Configuration* > *Policies* and do one of the following:
     - Create a new policy and select the security profile group.
     - Edit an existing policy and select the security profile group.
   - For SWG agentless remote users, go to *Configuration* > *SWG Policies* and do one of the following:
     - Create a new SWG policy and select the security profile group.
     - Edit an existing SWG policy and select the security profile group.

For details on security profile groups and configuring them in policies, see Security profile groups on page 145.

The following tables list the vendor-specific headers that you must configure in the inline-CASB headers page:

Microsoft Office 365

Header name	Header content	Example header content	Action	Destination
`Restrict-Access-To-Tenants`	Domains and tenant ID	`azure.domain.com, domain.com, d0cf12c3-456c-7e89-0d1e-03e456de78f9`	Add to request	Use the built-in *Microsoft Office* 365 address group.
`Restrict-Access-Context`	Directory ID	`d1cf23c4-567c-8e90-1d2e-03e456de78f9`		
`sec-Restrict-Tenant-Access-Policy`	`restrict-msa`	`restrict-msa`		Create a new custom address object for login.live.com

The built-in Microsoft Office 365 address group includes:

- login.microsoftonline.com
- login.microsoft.com
- login.windows.net

For proper functioning of Microsoft Office 365 tenant restrictions, you must include the tenant ID in addition to the domains in a comma-separated list configured for `Restrict-Access-To-Tenants`.

Google Workspace

Header name	Header content	Example header content	Action	Destination
`X-GoogApps-Allowed-Domains`	Domain	`mydomain1.com, mydomain2.com`	Add to request	Use the built-in G Suite address group.

The built-in G Suite address group includes:

- gmail.com
- wildcard.google.com (*.google.com)

Slack

Header name	Header content	Example header content	Action	Destination
`X-Slack-Allowed-Workspaces-Requester`	Workspace or organization ID representing your Business+ or	`xxxxxx`	Add to request	Create a new address object called wildcard.slack.com containing an FQDN

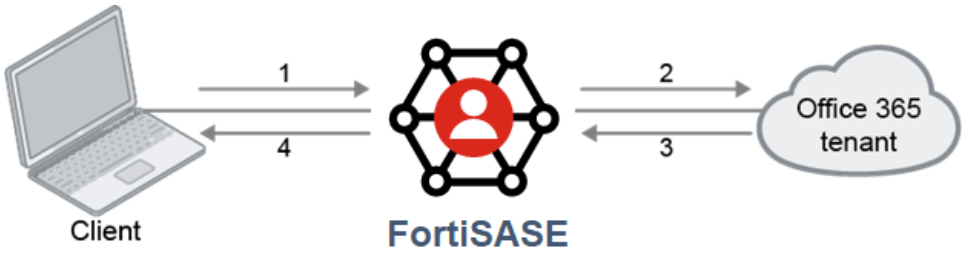
Header name	Header content	Example header content	Action	Destination
	Enterprise Grid account			of *.slack.com
`X-Slack-Allowed-Workspaces`	Organization IDs or workspace ID	`yyyyyy`		

You must manually create a new address object called wildcard.slack.com containing the FQDN of *.slack.com via the *Create* button when in the *Select Entries* slide-in resulting from clicking the *Destination* in the *Inline-CASB Header* slide-in.

Due to vendors' changing requirements, these settings may no longer comply with the vendors' official guidelines. See the vendor documentation in SaaS vendor-specific headers on page 178.

Configuring inline-CASB header for Office 365 example

This example creates inline-CASB headers in FortiSASE to control permissions for Microsoft Office 365 to allow corporate domains and deny personal accounts, such as Hotmail and Outlook, that a user accesses through login.live.com.



- When a user attempts to access login.microsoftonline.com, login.microsoft.com, or login.windows.net:
  - For a FortiClient agent-based remote user, the traffic will match a policy
  - For a SWG agentless remote user, the traffic will match a SWG policy.
    If this is the first time the user has attempted to access the internet, then the user must enter valid credentials for the SSO authentication prompt.
- The Web Filter with Inline-CASB adds new headers to the customer tenant, indicating the allowed domain and restricted access for personal accounts. Next, FortiSASE starts a new connection with the Microsoft Office 365 domain controller including the new headers.
- The Microsoft Office 365 domain controller assesses this data and will allow or deny this access, then sends a reply to FortiSASE.
- FortiSASE sends a reply to the client.

FortiSASE Web Filter with Inline-CASB will only indicate the correct domains to be allowed or denied through the headers to Microsoft. The custom sign-in portal in the browser is generated by Microsoft.

Inline-CASB headers configuration example

The `Restrict-Access-To-Tenants` and `Restrict-Access-Context` headers are inserted for incoming requests to: login.microsoftonline.com, login.microsoft.com, and login.windows.net, which are part of the Microsoft Office 365 address group.

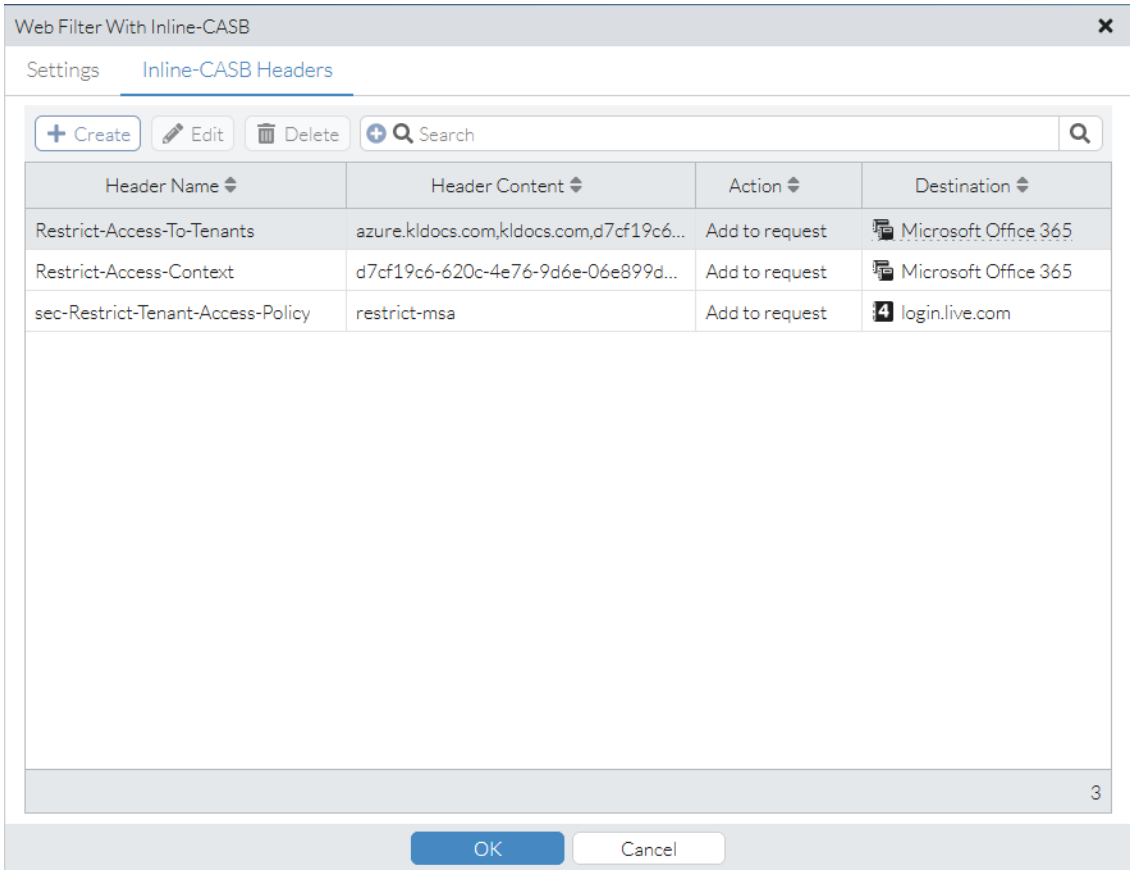
To restrict access to personal accounts using the login.live.com domain, the `sec-Restrict-Tenant-Access-Policy` header is inserted and uses `restrict-msa` as the header content.

Before configuring FortiSASE, collect the information related to the company domain in the Office 365 contract:

Header	Company domain-specific information
`Restrict-Access-To-Tenants`	• <domain.com> • Tenant ID
`Restrict-Access-Context`	Directory ID
`sec-Restrict-Tenant-Access-Policy`	`restrict-msa`

For proper functioning of Microsoft Office 365 tenant restrictions, you must include the tenant ID in addition to the domains in a comma-separated list configured for `Restrict-Access-To-Tenants`.

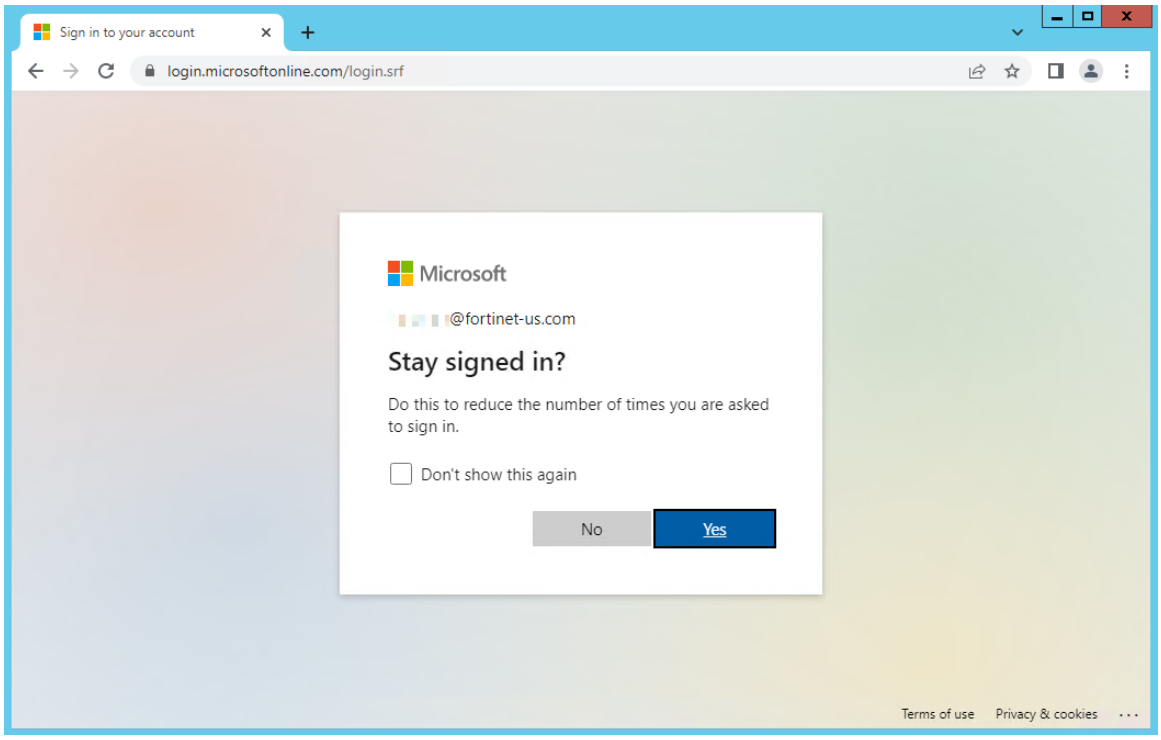
Following is an example of completed configuration in the *Inline-CASB Headers* tab within the *Web Filter with Inline-CASB* slide-in:



To test the access to corporate domains and personal accounts:

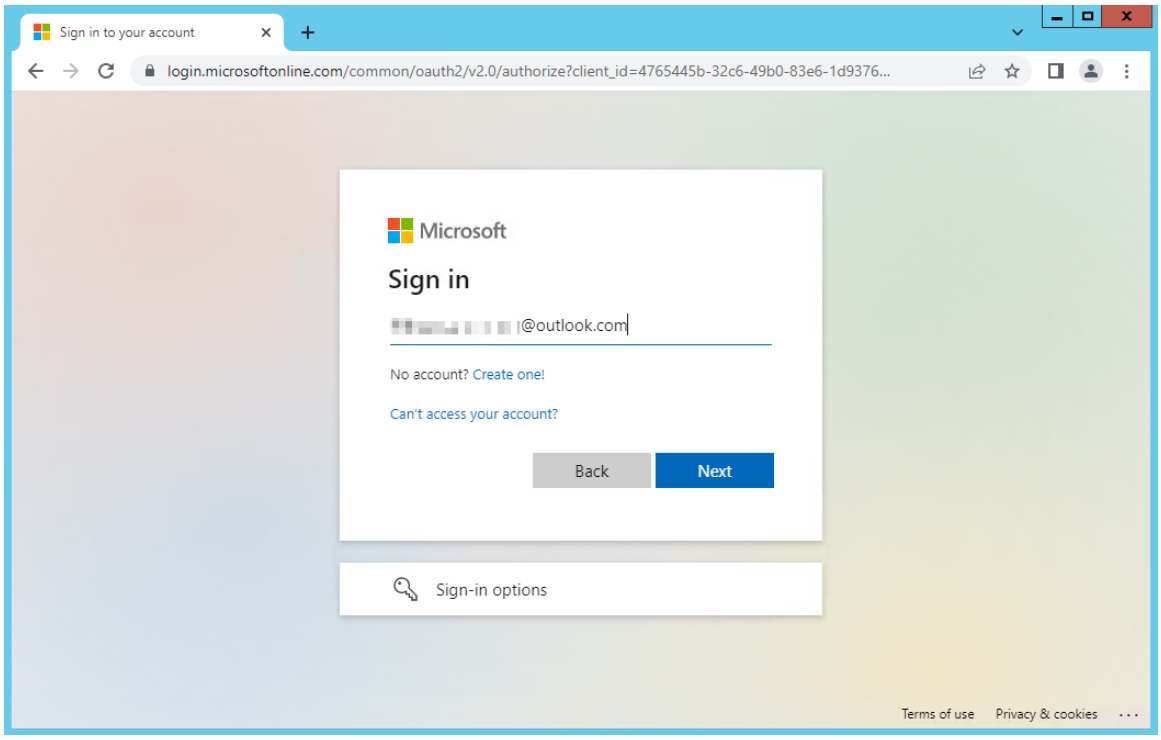
This section outlines the steps for testing the access with a client using a SWG agentless remote user. The steps are similar with a client using a FortiClient agent-based remote user.

1. Get a client to log in with their corporate email using the login.microsoftonline.com domain.



2. The client can enter their credentials and log in successfully.

3. Get a client to log in to their personal Outlook account.



4. After the client enters their credentials, a message appears that they cannot access this resource because by the cross-tenant access policy restricts it.
5. Try to log in using another corporate email with Microsoft 365 access that is from a domain not allowed on this tenant and observe the message about external access being blocked by policy.

To verify customized inline-CASB headers in security logs:

1. In FortiSASE, go to *Analytics* > *Security* > *Web Filter With Inline-CASB* to view the corresponding logs.
2. Right-click a table heading and add *Change Headers* to make HTTP headers visible.
3. Drag and drop the *Change Headers* heading to the left to make it easy to see without scrolling.
4. Click a log entry of interest and click *Details* to drill down to see details.

DNS Filter

You can apply DNS category filtering to control user access to web resources. DNS filtering has the following features:

Feature	Description
FortiGuard filtering	Filters the DNS request based on the FortiGuard domain rating. This makes use of FortiGuard's continuously updated domain rating database for more reliable protection.

Feature	Description
Botnet C&C domain blocking	Blocks the DNS request for the known botnet C&C domains. FortiGuard continually updates the botnet C&C domain list. The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage. This provides additional protection for your network.
Domain filter	Allows you to define your own domain list to block or allow. In a DNS filter profile, the local domain filter has a higher priority than FortiGuard category-based domain filter. DNS queries are scanned and matched first with the local domain filter. If an entry matches and the local filter action is set to block, then that DNS query is blocked and redirected. If the local domain filter list has no match, then the FortiGuard category-based domain filter is used. If a DNS query domain name rating belongs to the block category, the query is blocked and redirected. If the FortiGuard category-based filter has no match, then the original resolved IP address is returned to the client DNS resolver. If the local domain filter action is set to allow and an entry matches, it will skip the FortiGuard category-based domain filter and directly return to the client DNS resolver. If the local domain filter action is set to monitor and an entry matches, it will go to the FortiGuard category-based domain filter for scanning and matching.
DNS translation	Maps the resolved result to another IP address that you have defined.

Feature		Description
		For example, website A has a public address of 1.2.3.4. However, when your internal network users visit this website, you want them to connect to the internal host 192.168.3.4. You can use DNS translation to translate the DNS resolved address 1.2.3.4 to 192.168.3.4. Reverse use of DNS translation is also applicable. For example, if you want a public DNS query of your internal server to get a public IP address, then you can translate a DNS resolved private IP to a public IP address.
Options	Redirect botnet C&C requests to Block Portal	FortiGuard Service continually updates the botnet C&C domain list. The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage.
	Log all DNS queries and responses	Enable to log all domains visited (detailed DNS logging).
	Allow DNS requests when a rating error occurs	Enable to allow all domains when FortiGuard DNS servers fail, or they are unreachable from FortiSASE. When this happens, a log message is recorded in the DNS logs by default.
	Enforce 'Safe Search' on Google, Bing, YouTube	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

For individual search engine safe search specifications, refer to the documentation for Google, Bing, and YouTube.

To configure a DNS Filter profile:

1. Go to *Security Profiles* > *Configuration*.
2. Enable *DNS Filter*.
3. Click *Customize*.
4. To configure FortiGuard filtering, do the following:
   a. Enable *FortiGuard Category Based Filter*.
   b. Select the desired category, then select the desired action: *Allow*, *Monitor*, or *Redirect Block Portal*.

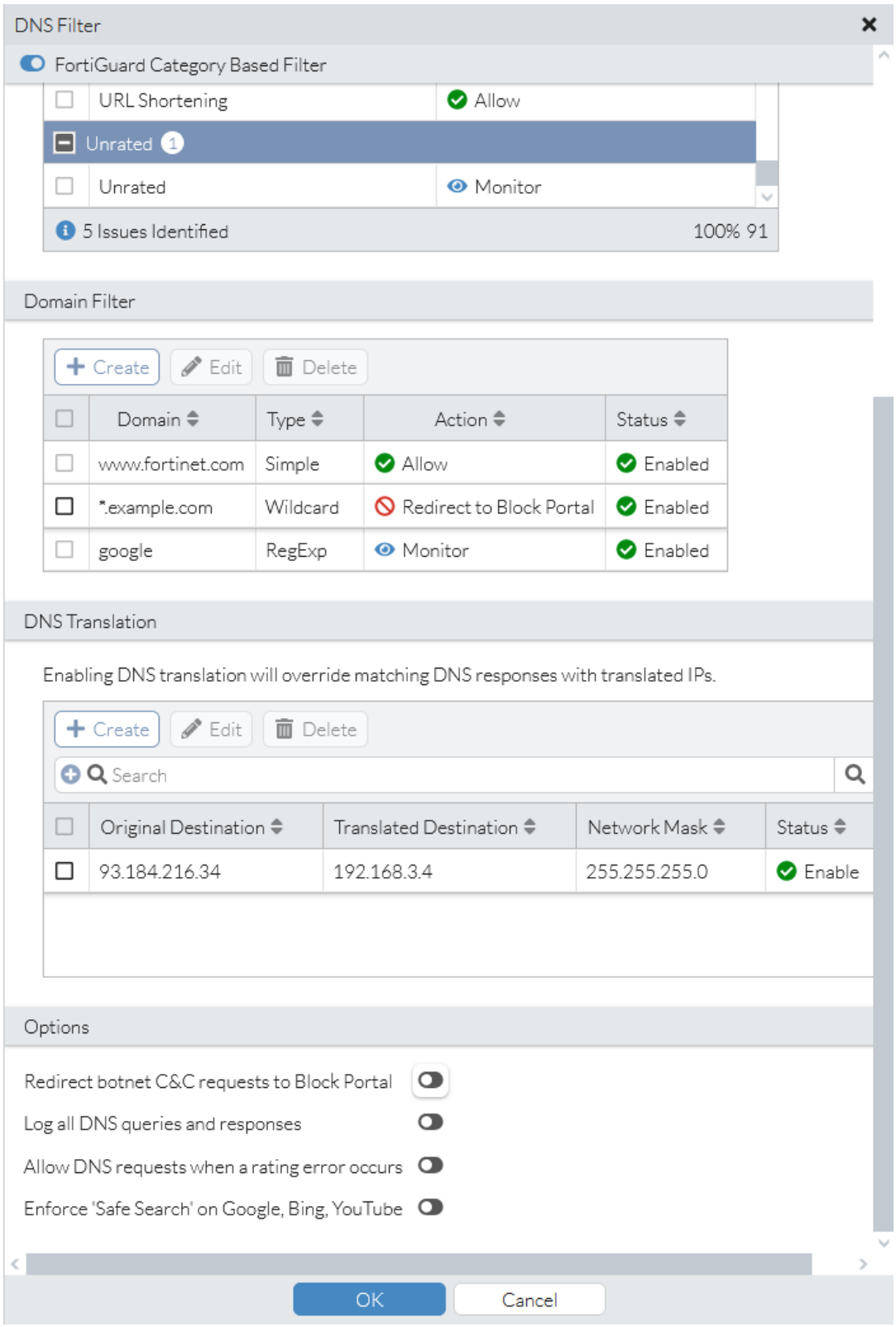
c. If desired, click *Manage Categories*. Select the desired category, then click *Edit*. You can enable and configure the *Threat Level* for the category. You must configure a threat level for this category to appear in FortiView Threats after the DNS filter blocks it.

5. To configure domain filter, do the following:
   a. Click *Create* under *Domain Filter*.
   b. Enter a domain, and select a *Type* and *Action*.
   c. Click *OK*. The example has configured three domain filters:

Domain	Type	Action
www.fortinet.com	Simple	Allow
*.example.com	Wildcard	Redirect to Block Portal
google	Regular expression	Monitor

6. To configure DNS translation, do the following:
   a. Under *DNS Translation*, click *Create*.
   b. In the *Original Destination* field, enter the domain's original IP address. For example, if you want the DNS filter profile to translate 93.184.216.34 (www.example.com) to 192.168.3.4, you would configure the original destination as 93.184.216.34.
   c. In the *Translated Destination* field, enter the translated destination IP address. For the example, you would enter 192.168.3.4 as the translated destination.
   d. In the *Network Mask* field, enter the desired network mask.
   e. Click *OK*. With this configuration, when an internal network user performs a DNS query for www.example.com, they do not get the original www.example.com IP address of 93.184.216.34. Instead, the DNS filter replaces it with 192.168.3.4.
7. To configure *Options*, do the following:
   a. To enable botnet C&C domain blocking, enable *Redirect botnet C&C requests to Block Portal*. If desired, you can click the botnet package link to view the latest list of botnet C&C domain definitions.
   b. If desired, enable *Log all DNS queries and responses*. You can view these logs in *Analytics* > *Security* > *DNS Filter*.
   c. If desired, enable *Allow DNS requests when a rating error occurs*. When FortiGuard DNS servers fail, or they are unreachable from FortiSASE, allow DNS requests from all domains and record a log message in *Analytics* > *Security* > *DNS Filter*.
   d. If desired, enable *Enforce 'Safe Search' on Google, Bing, YouTube* to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

8. Click *OK*.


DNS Filter
FortiGuard Category Based Filter
URL Shortening
Allow
Unrated 1
Unrated
Monitor
5 Issues Identified
100% 91
Domain Filter
Create
Edit
Delete
Domain
Type
Action
Status
www.fortinet.com
Simple
Allow
Enabled
*.example.com
Wildcard
Redirect to Block Portal
Enabled
google
RegExp
Monitor
Enabled
DNS Translation
Enabling DNS translation will override matching DNS responses with translated IPs.
Create
Edit
Delete
Search
Original Destination
Translated Destination
Network Mask
Status
93.184.216.34
192.168.3.4
255.255.255.0
Enable
Options
Redirect botnet C&C requests to Block Portal
Log all DNS queries and responses
Allow DNS requests when a rating error occurs
Enforce 'Safe Search' on Google, Bing, YouTube
OK
Cancel

Enforcing safe search in DNS filter

To enforce safe search, you must use SSL deep inspection. See Certificate and deep inspection modes on page 146.

To enforce safe search in DNS filter:

1. Go to *Configuration* > *Security*.
2. Create a new profile group by clicking on the dropdown next to *Profile Group* and clicking the plus sign (+) or select an existing profile group.
3. Enable *DNS Filter*.
4. Under *DNS Filter*, click *Customize*.
5. Scroll down to the *Options* section and enable *Enforce 'Safe Search' on Google, Bing, YouTube*.
6. Click *OK*.

For individual search engine safe search specifications, refer to the documentation for Google, Bing, and YouTube.

To validate safe search after enforcing it in DNS filter:

You can use a tool such as dig or nslookup to demonstrate that the domain lookup for a search site has been replaced by its safe search equivalent site.

1. On a Windows endpoint in the Windows Command Prompt, run nslookup for Google and observe the following output:

```
nslookup google.com
...
Non-authoritative answer:
Name:    forcesafesearch.google.com
Addresses:  2001:4860:4802:32::78
216.239.38.120
Aliases:  google.com
```

2. On a Windows endpoint in the Windows Command Prompt, run nslookup for Bing and observe the following output:

```
nslookup bing.ca
...
Non-authoritative answer:
Name:    strict.bing.com
Address:  204.79.197.220
Aliases:  bing.ca
```

3. On a Windows endpoint in the Windows Command Prompt, run nslookup for YouTube and observe the following output:

```
nslookup youtube.com

...

Non-authoritative answer:

Name:    restrict.youtube.com

Addresses:  2001:4860:4802:32::78

216.239.38.120

Aliases:  youtube.com
```

Application Control With Inline-CASB

FortiSASE can recognize network traffic that a large number of applications generate. Application Control With Inline-cloud access security broker (Inline-CASB) uses Intrusion Prevention System (IPS) protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Application Control With Inline-CASB supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0).

FortiSASE uses Application Control and SSL deep inspection to act as an Inline-CASB by providing access control to software-as-a-service (SaaS) cloud application traffic. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

Application Control With Inline-CASB features are not guaranteed to work when other security features are disabled. Enabling one of the following security features is recommended: Antivirus, File filter, DLP, Web filter, or DNS filter.

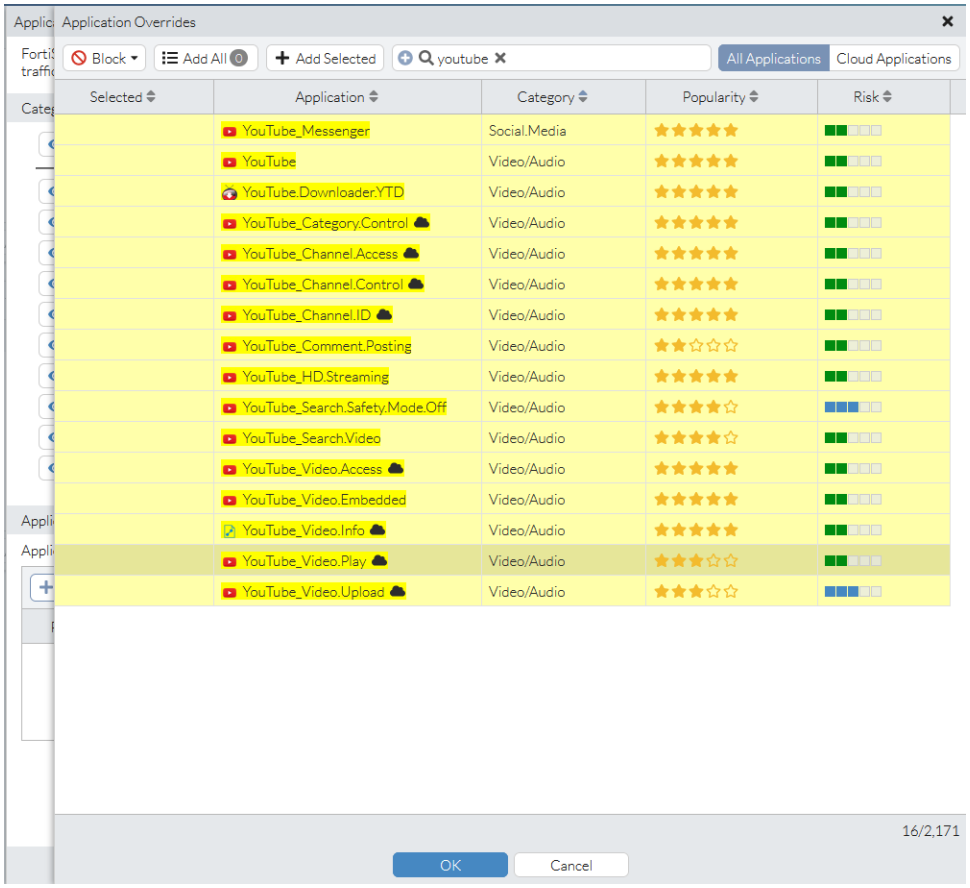
To configure Application Control With Inline-CASB:

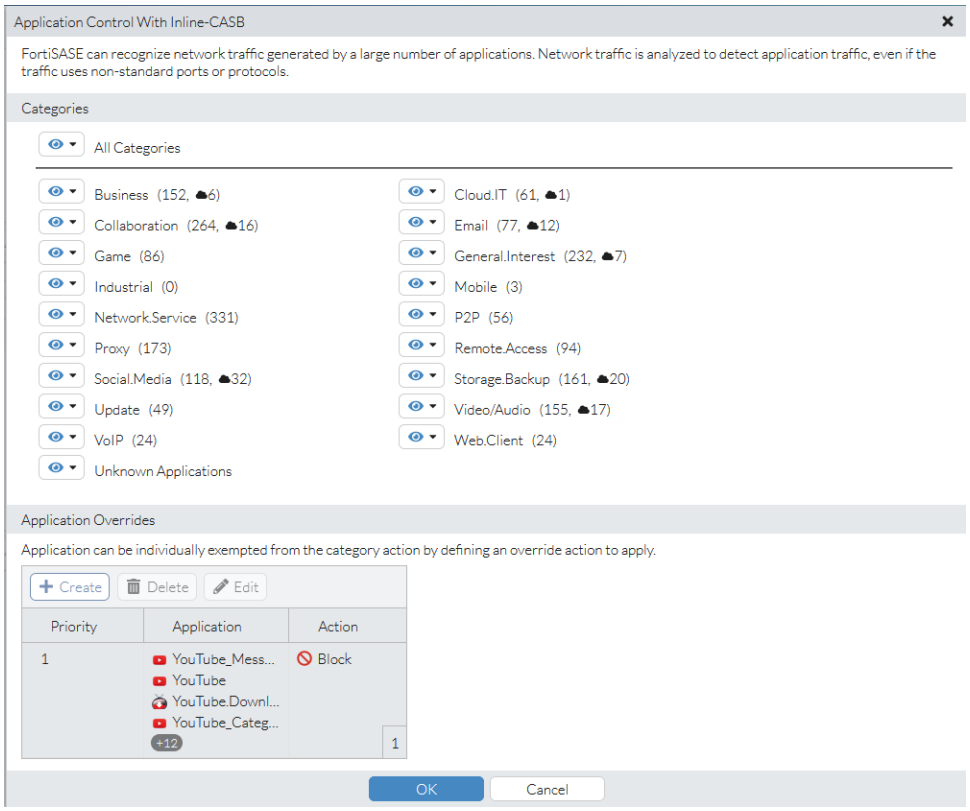
1. Go to *Configuration* > *Security*.
2. Enable *Application Control With Inline-CASB*.
3. In the *Application Control With Inline-CASB* widget, click *Customize*.
4. The *Application Control With Inline-CASB* pane displays the application categories. You can configure one of the following actions for each category:

Type	Description
Allow	Passes the traffic to the web filters, antivirus inspection engine, and DLP inspection engine.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies or blocks attempts to access any application that belongs to the category. A replacement message displays.

5. In *Application Overrides*, you can configure actions for individual applications, overriding the action configured for their category. Click *Create*. Select the desired action from the dropdown list in the upper left corner, select the

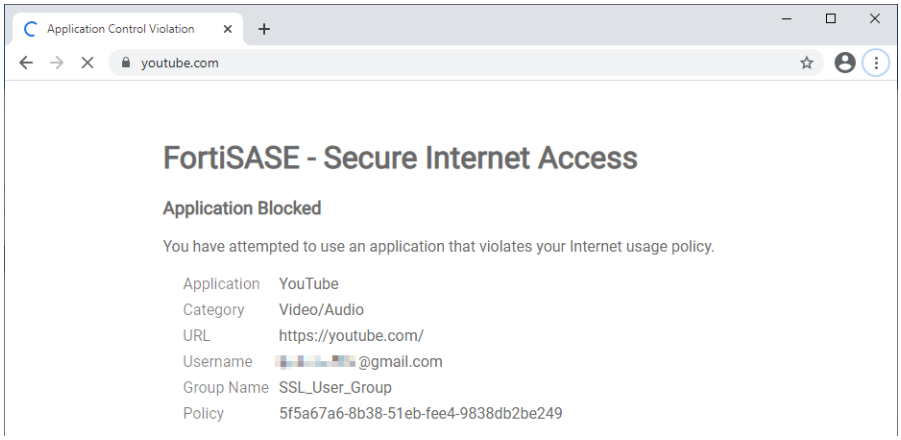
desired applications, then click *OK*. You can search for the desired applications, and filter the list to show only cloud applications. The *Application Overrides* pane denotes cloud applications with a cloud icon, such as for the YouTube_Category.Control application in the following screenshot. The following example allows the Video/Audio category, and blocks YouTube.





6. Click *OK*.

When the user attempts to access YouTube under these settings, they see the following message in their browser.



You can view data for cloud application access attempts in *Dashboards* > *FortiView Cloud Applications*.

Profile resources

The *Profile resources* tab is available on the toolbar under *Configuration* > *Security*. It consists of options to configure custom IPS signatures, FortiGuard categories, and custom Web Filter categories that are shared and available across different security profile groups.

To create, edit, and delete a custom IPS signature:

1. Go to *Configuration* > *Security*.
2. Select the *Profile resources* tab from the toolbar.
3. Select *Custom IPS signatures* to see all custom IPS signatures created across different security profile groups.
4. Do one of the following:
   - To create an IPS signature, click *Create*. In the slide-in, specify *Tag*, *Comments*, and *Signature* using Creating IPS and application control signatures. Click *OK*. The newly created IPS signature is available to use in the *Intrusion Prevention* widget across different security profiles.
   - To edit an IPS signature, select the desired IPS signature and click *Edit*. After making the required edits, click *OK*.
   - To delete, select the desired IPS signature available in the *Custom IPS signatures* list and click *Delete*. On the *Confirm delete* prompt, click *OK*.

To edit FortiGuard category threat levels:

1. Go to *Configuration* > *Security*.
2. On the *Profile resources* tab, select *FortiGuard categories*.
3. Click desired FortiGuard category from the list and click *Edit*.
4. Enable the *Threat level* toggle and select the appropriate level as per your requirement.
5. Click OK.

To create Custom Web Filter Category from Profile resources:

1. Go to *Configuration* > *Security*.
2. On the *Profile resources* tab, select *Custom Web Filter categories*. Two default custom categories, custom1 and custom2, are available to use across different security profile groups.
3. To edit a default custom category, do the following:
   a. Select *custom1* or *custom2* and click *Edit*.
   b. Specify the desired URLs and configure the threat level for the default custom category. Click *OK*.
4. To create a new category, do the following:
   a. Click *Create Custom Category*.
   b. Specify the desired *Name*, *URLs*, and *Threat Level* for the custom category.
   c. Click *OK*. These custom categories are available to use in Web Filter settings across different security profile groups.

External feeds

You can configure external feeds on FortiSASE to dynamically import an external list from an HTTP/HTTPS server hosted in the form of a plain text file. The imported list is then available as an external feed and you can use it to enforce special security requirements, such as long-term policies to always allow or block access to certain websites or short-term requirements to block access to known compromised locations. The external feeds are dynamically synchronized and updated periodically at the configured refresh rate so that any changes in entries of external list are immediately imported to FortiSASE.

FortiSASE supports the following external feed types:

External feed type	File description	Example format
External hosts	One IP address, IP address range, or subnet address per line. An address can be IPv4 or IPv6. You do not need to enter an IPv6 address in [ ] format.	192.168.2.100 172.200.1.4/16 172.16.1.2/24 172.16.8.1-172.16.8.100 2001:0db8::eade:27ff:fe04:9a01/120 2001:0db8::eade:27ff:fe04:aa01-2001:0db8::eade:27ff:fe04:ab01
DNS filter domains	One domain per line. Supports simple wildcards and international domain names.	mail.*.example.com *-special.example.com www.*example.com example.com
Web filter FQDNs	One URL per line.	http://example/com.url https://example.com/url http://example.com:8080/url

Consider the following file format requirements for an external resources files:

- In plain text format with each URL list, IP address, and domain name occupying one line.
- Limited to 10 MB or 128 × 1024 (131072) entries, whichever limit is hit first.
- There is no duplicated entry validation for the external resources file (entry inside each file or inside different files).
- If the number of entries exceeds the limit, FortiSASE does not load additional entries beyond the threshold.

You can set the external resources update period by configuring *Refresh rate*.

FortiClient blocks IPv6 traffic and it does not traverse through the FortiSASE tunnel. External feeds only support listing IPv6 addresses for external feed interoperability with different devices, but FortiSASE does not support IPv6 traffic traversal.

Configuring an external feed

You can configure a maximum of 20 external feeds of the same or different types. Depending on their type, you can use external feeds to configure traffic or secure web gateway policies, DNS filter, or Web Filter to allow or deny access to network resources that the information retrieved from the external feed specifies.

To configure a feed:

1. Go to *Configuration* > *External feeds*. Click *Create*.
2. In the *New External Feed* page, configure the following:

Field	Value
Name	Enter a unique name.
Comments	(Optional) Add a comment.

Field	Value
Status	Enable or disable the feed.
Refresh rate	Enter a value from 1 to 43200 in minutes as per your requirement.
Feed type	Select feed type from the following: • External hosts • DNS filter domains • Web filter FQDNs
URI	Select a protocol for FortiSASE to use to access the external feed: • http:// • https://
HTTP basic authentication	(Optional) Enable or disable basic HTTP authentication. When enabled, enter the username and password in the requisite fields.
Block in Threat Feed Deny policy	Available for external hosts feed. When you enable this option, FortiSASE automatically adds this feed in the *Destination* field for the default Threat Feed Deny policy blocking access for secure internet access traffic. **To view the feed in Threat Feed Deny policy:** • For agent-based endpoints, go to *Configuration* > *Policies* > *Threat Feed Deny*. View the *Destination* field. • For agentless endpoints, go to *Configuration* > *SWG Policies* > *Threat Feed Deny*. View the *Destination* field.
Block in default internet access profile group	Available for DNS filter domains and Web filter FQDNs feed. When you enable this option, FortiSASE automatically adds this feed with an *Action* of *Block* in the default internet access profile group. **To view the block action for the feed:** 1. Go to *Configuration* > *Security* and select the Default profile group. 2. Do one of the following: • For a DNS filter domains feed, under *DNS Filter*, click *Customize*. Under *FortiGuard Category Based Filter*, view the *Domain feeds* category. • For a web filter FQDNs feed, under *Web Filter With Inline-CASB*, click *Customize*. Under *FortiGuard Category Based Filter*, view *FQDN feeds*.

3. Click *OK*. The feed is visible under *Configuration* > *Feed*.

Applying an external feed

To apply an external host feed:

You can use an external host feed as the source or destination for a traffic or secure web gateway policy for secure internet access (SIA) and secure private access traffic (SPA).

1. Do one of the following:
   - Go to *Configuration* > *Policies*.
   - Go to *Configuration* > *SWG Policies*.
2. Select the desired policy, then click *Edit*.
3. In the *Source/Destination* field, click *Specify*.
4. From the *Select Entries* slide in, select the required external feed under *External threat feeds*. Click *Close*.
5. Specify the policy action as *Accept* or *Deny* as per your need.
6. Click *OK*.

To apply a DNS filter domain feed:

You can use a DNS filter domain feed as a domain feed category in *DNS Filter*.

1. Go to *Configuration* > *Security*. Select the appropriate *Profile Group* from the dropdown in the top right corner.
2. Go to *DNS Filter* and click *Customize*.
3. In the slide in, a *Domain feeds* category appears under *FortiGuard Category Based Filter*, which shows all the configured DNS filter domain feeds. Click the required DNS filter domain feed and select the appropriate action:

Action	The DNS request is...	Security log generated under *Analytics* > *Security* > *DNS Filter*?
Allow	Allowed to pass	No
Monitor	Allowed to pass	Yes
Redirect to Block Portal	Blocked. Returns a FortiGuard block page	Yes

4. Click *OK*.
5. Do one of the following under *Internet Access* (SIA) or *Private Access* (SPA):
   - For agent-based users, go to *Configuration* > *Policies*.
   - For agentless users, go to *Configuration* > *SWG Policies*.
6. Select the required policy and click *Edit*.
7. In the *Profile Group* field, select the profile group that has *DNS filter domain feed* configured
8. Click *OK*.

To apply a web filter FQDN feed:

You can use a web filter FQDN feed as a web filter FQDN feed category.

1. Go to *Configuration* > *Security*. Select the appropriate *Profile Group* from the dropdown in the top right corner.
2. Go to *Web Filter With Inline-CASB* and click *Customize*.
3. In the slide in, a *FQDN feeds* category appears under *FortiGuard Category Based Filter*, which shows all the configured Web filter FQDN feeds. Click the required FQDN feed and select the appropriate action:

Action	Description
Allow	Permit access to websites in the .
Monitor	Permit and log access to websites in the category.

Action	Description
Block	Prevent access to websites in the category. Users trying to access a blocked site see a replacement message indicating that FortiSASE blocks the site.
Warning	Display a message to the user allowing them to continue if they choose.
Disable	Remove the category from the from the web filter profile. This option is only available for local or remote categories from the right-click menu.

4. Click *OK*.
5. Do one of the following under *Internet Access* (SIA) or *Private Access* (SPA):
   - For agent-based users, go to *Configuration* > *Policies*.
   - For agentless users, go to *Configuration* > *SWG Policies*.
6. Select the required policy and click *Edit*.
7. In the *Profile Group* field, select the profile group that has *Web filter FQDN feed* configured.
8. Click *OK*.

Authentication Sources and Access

In *Authentication Sources* and *Access*, you can control network access for different users and devices in your network. FortiSASE authentication controls system access by user group. By assigning individual users to the appropriate user groups, you can control each user's access to network resources. You can define local users and remote users in FortiSASE. You can also integrate user accounts on remote authentication servers and connect them to FortiSASE.

The following summarizes the provisioning process for different user types on FortiSASE:

User type	Provisioning process
LDAP	Configure remote users over LDAP to easily integrate FortiSASE with a Windows Active Directory (AD) server or another LDAP server. You can invite users in one of the following ways: • Define an individual user and send the invitation to them directly • Create a user group and send the invitation using the *Onboard Users* button See Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode on page 199. See Configuring FortiSASE with an LDAP server for remote user authentication in SWG agentless mode on page 203.
RADIUS	Configure remote authentication with a RADIUS server. You can allow all users from the IdP or define a group in *Configuration* > *Users*. Send the invitation code to users using the *Onboard Users* button. See Configuring FortiSASE with a RADIUS server for remote user authentication on page 207.

User type	Provisioning process
Single sign on (SSO)	Configure an SSO connection with an authentication server such as Entra ID or Okta, where Entra ID or Okta is the identity provider (IdP) and FortiSASE is the service provider (SP). You can allow all users from the IdP or define a group in *Configuration* > *Users*. Send the invitation code to users using the *Onboard Users* button. See: • Configuring FortiSASE with Entra ID SSO in FortiClient agent-based mode on page 211 • Configuring FortiSASE with Entra ID SSO in SWG agentless mode on page 218 • Configuring FortiSASE with Okta SSO on page 226.
Local	Define user in *Configuration* > *Users* and send invitation to them directly. See Users on page 242.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

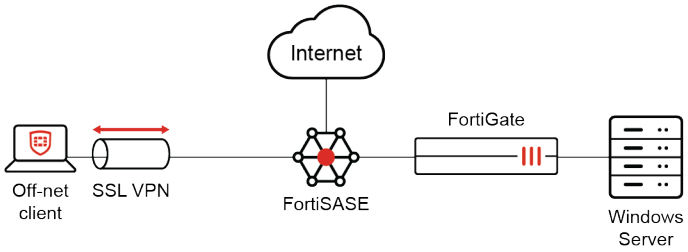
The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

The *Onboard Users* button, which is available from the *Remote User Management* widget on the *Status* dashboard, allows you to send an email to users to invite them to FortiSASE. They can register their FortiClient to FortiClient Cloud by using the instructions in the invitation email. You must still provision users via one of the aforementioned methods to give them access to VPN and other FortiSASE resources.

Configuring FortiSASE with an LDAP server for remote user authentication in FortiClient agent-based mode

LDAP authentication is not available for remote VPN users using IPsec VPN.

Configuring remote users over LDAP allows FortiSASE to easily integrate with a Windows Active Directory (AD) server or another LDAP server. This example has a Windows domain controller that has users defined in its AD. You want to allow certain users VPN access over FortiSASE. These users connect using their Windows domain credentials.



The Windows server is protected by a FortiGate that uses a virtual IP address (VIP) to port forward port 10636 to the Windows server. Communication over this VIP is allowed only for the FortiSASE IP address. The example domain is KLHOME.local.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

Configuring the LDAP server in FortiSASE

To configure the LDAP server in FortiSASE:

1. Go to *Configuration* > *LDAP*.
2. Click *Create*.
3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the LDAP server. Ensure the SPA network is configured.
Server IP/Name	LDAP server IP address or FQDN.
Server Port	By default, LDAP uses port 636 and a secure connection. If you are using a custom port, define it here. In this example, it is 10636.
Common Name Identifier	This is the attribute in which your LDAP server identifies the username. • In an AD, this is commonly the common name attribute, which is denoted

Field	Description
	`cn`. • Alternatively, you can use `sAMAccountName`. This is case-sensitive. • In other LDAP servers, it may be the user ID, which is denoted `uid`. • In an AD, for usernames in the username@domain format, use the user principal name (UPN) attribute, which is denoted `userPrincipalName`.
Distinguished Name	Used to look up user account entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the CN identifier in which you are doing the lookup. If you want to recursively look up all objects under the root domain in the example AD, specify `dc=KLHOME,dc=local`. If you want to look up users under a specific organization unit, specify `ou=VPN-Users,dc=KLHOME,dc=local`.
Secure Connection	Enable to connect to server by LDAPS by default. Using LDAPS is recommended to ensure an encrypted connection. If disabled, communication occurs in clear text.
Password Renewal	Enable remote password renewal. When the LDAP user's password expires, the user can renew their password when authenticating with FortiSASE. This option is only available if using LDAPS.
Certificate	Select the CA certificate for your LDAPS connection. If this certificate is not signed by a known CA, you must export the certificate from your server and install this on FortiSASE. To import the certificate, do the following: 1. Click *Certificate*, then *Create*. 2. If you have the certificate file, select *File*. 3. Click *Upload*. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in *System* > *Certificates*.
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the *Server IP/Name* field.
Advanced Group Matching	Enable advanced group matching. Based on your LDAP server, you may need to configure additional properties to ensure that FortiSASE correctly matches LDAP groups.
Group Member Check	Determines which attributes FortiSASE uses for group matching: • Group object • POSIX group object • User attribute
Group Filter	Enter the filter to use for group matching. Required when *Group Member Check* is set to User attribute.
Group Search Base	Enter the search base to use for group searching. Required when *Group Member Check* is set to User attribute.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

4. Configure the following *Authenticate* settings:

Field	Description
Bind Type	Select one of the following. Regular bind is recommended: • **Simple**: bind using simple password authentication using the client name. The LDAP server only looks up against the distinguished name (DN), but does not search on the subtree. • **Anonymous**: bind using anonymous user and search starting from the DN and recurse over the subtrees. Many LDAP servers do not allow this. • **Regular**: bind using username/password provided and search starting from the DN and recurse over the subtrees.
Username	If using regular bind, enter the username. In the example AD, this may be `KLHOME\administrator` or `administrator@KLHOME`.
Password	If using regular bind, enter the password.
Client Certificate	Enable client certificate for authentication with LDAPS server. Select the client certificate that you previously uploaded to FortiSASE.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the LDAP server, or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

Configuring remote users from the LDAP server

To configure remote users from the LDAP server:

1. Do one of the following:
   - To send invitations directly to individual users, do the following:
     i. Go to *Configuration* > *Users*.
     ii. Click *Create*.
     iii. Select *LDAP User*, then click *Next*.
     iv. From the *LDAP Server* dropdown list, select the server that you configured. Click *Next*.
     v. FortiSASE displays the available remote users. It displays all users starting from the DN root to the subtrees. Select users as desired. Click *Next*.
     vi. Provide the users' email addresses. FortiSASE sends invitation codes and connection instructions to these email addresses.
     vii. Click *OK*.
   - To create and send invitations to a group of users, do the following:
     i. Go to *Configuration* > *Users*.
     ii. Click *Create* > *User Group*.
     iii. In the *Users* field, click +.
     iv. In the *Select Entries* pane, select the desired users to add to this user group.

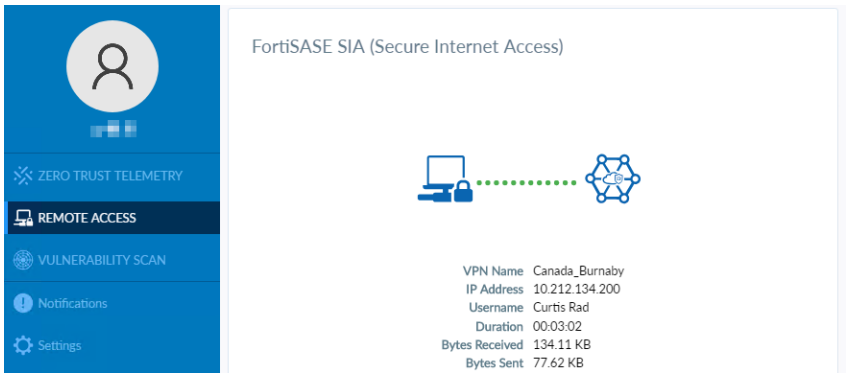
v. In the *Remote Groups* field, select *Create*.
vi. From the *Remote Server* dropdown list, select the desired server.
vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK* twice.
viii. Go to *Dashboards* > *Status*. In the *Remote User Management* widget, click *Onboard Users*.
ix. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Connecting VPN from FortiClient

The end user follows these instructions to connect to the FortiSASE VPN tunnel.

To connect VPN from FortiClient:

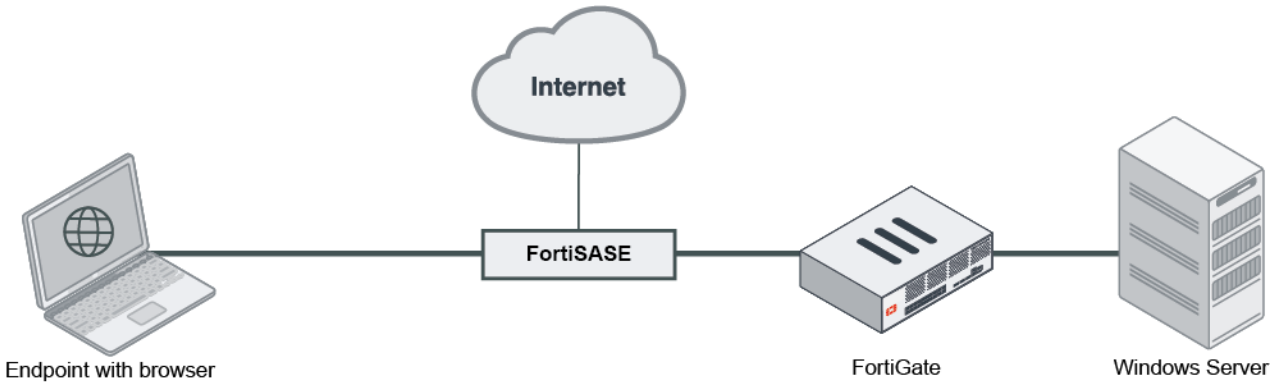
1. Follow the instructions from the received email to install the compatible FortiClient version on to your device.
2. Once installed, open FortiClient.
3. On the *ZERO TRUST TELEMETRY* tab, in the *Join FortiClient Cloud* field, enter the invitation code from the received email.
4. FortiClient connects to and becomes provisioned by FortiClient Cloud. On the *REMOTE ACCESS* tab, connect to the preconfigured VPN tunnel using your Windows username and password. If the administrator configured the CN identifier as `cn`, the username is likely the user's full name. Once connected, the *REMOTE ACCESS* tab displays the active VPN connection and additional information.



Configuring FortiSASE with an LDAP server for remote user authentication in SWG agentless mode

FortiSASE performs secure web gateway (SWG) authentication via HTTP. Therefore, single sign on (SSO) authentication is strongly recommended for SWG users, see Configuring FortiSASE with Entra ID SSO in SWG agentless mode on page 218.

Configuring remote users over LDAP allows FortiSASE to easily integrate with a Windows Active Directory (AD) server or another LDAP server. This example has a Windows domain controller that has users defined in its AD. You want to allow certain users to configure FortiSASE as their SWG server. These users authenticate using their Windows domain credentials.



The Windows server is protected by a FortiGate that uses a virtual IP address (VIP) to port forward port 10636 to the Windows server. Communication over this VIP is allowed only for the FortiSASE IP address. The example domain is KLHOME.local.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

Configuring the LDAP server in FortiSASE

To configure the LDAP server in FortiSASE:

1. Go to *Configuration* > *LDAP*.
2. Click *Create*.
3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the LDAP server. Ensure the SPA network is configured.
Server IP/Name	LDAP server IP address or FQDN.
Server Port	By default, LDAP uses port 636 and a secure connection. If you are using a custom port, define it here. In this example, it is 10636.
Common Name Identifier	This is the attribute in which your LDAP server identifies the username. • In an AD, this is commonly the common name attribute, which is denoted

Field	Description
	`cn`. • Alternatively, you can use `sAMAccountName`. This is case-sensitive. • In other LDAP servers, it may be the user ID, which is denoted `uid`. • In an AD, for usernames in the username@domain format, use the user principal name (UPN) attribute, which is denoted `userPrincipalName`.
Distinguished Name	Used to look up user account entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the CN identifier in which you are doing the lookup. If you want to recursively look up all objects under the root domain in the example AD, specify `dc=KLHOME,dc=local`. If you want to look up users under a specific organization unit, specify `ou=VPN-Users,dc=KLHOME,dc=local`.
Secure Connection	Enable to connect to server by LDAPS by default. Using LDAPS is recommended to ensure an encrypted connection. If disabled, communication occurs in clear text.
Password Renewal	Enable remote password renewal. When the LDAP user's password expires, the user can renew their password when authenticating with FortiSASE. This option is only available if using LDAPS.
Certificate	Select the CA certificate for your LDAPS connection. If this certificate is not signed by a known CA, you must export the certificate from your server and install this on FortiSASE. To import the certificate, do the following: 1. Click *Certificate*, then *Create*. 2. If you have the certificate file, select *File*. 3. Click *Upload*. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in *System* > *Certificates*.
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the *Server IP/Name* field.
Advanced Group Matching	Enable advanced group matching. Based on your LDAP server, you may need to configure additional properties to ensure that FortiSASE correctly matches LDAP groups.
Group Member Check	Determines which attributes FortiSASE uses for group matching: • Group object • POSIX group object • User attribute
Group Filter	Enter the filter to use for group matching. Required when *Group Member Check* is set to User attribute.
Group Search Base	Enter the search base to use for group searching. Required when *Group Member Check* is set to User attribute.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

4. Configure the following *Authenticate* settings:

Field	Description
Bind Type	Select one of the following. Regular bind is recommended: • **Simple**: bind using simple password authentication using the client name. The LDAP server only looks up against the distinguished name (DN), but does not search on the subtree. • **Anonymous**: bind using anonymous user and search starting from the DN and recurse over the subtrees. Many LDAP servers do not allow this. • **Regular**: bind using username/password provided and search starting from the DN and recurse over the subtrees.
Username	If using regular bind, enter the username. In the example AD, this may be `KLHOME\administrator` or `administrator@KLHOME`.
Password	If using regular bind, enter the password.
Client Certificate	Enable client certificate for authentication with LDAPS server. Select the client certificate that you previously uploaded to FortiSASE.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the LDAP server, or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

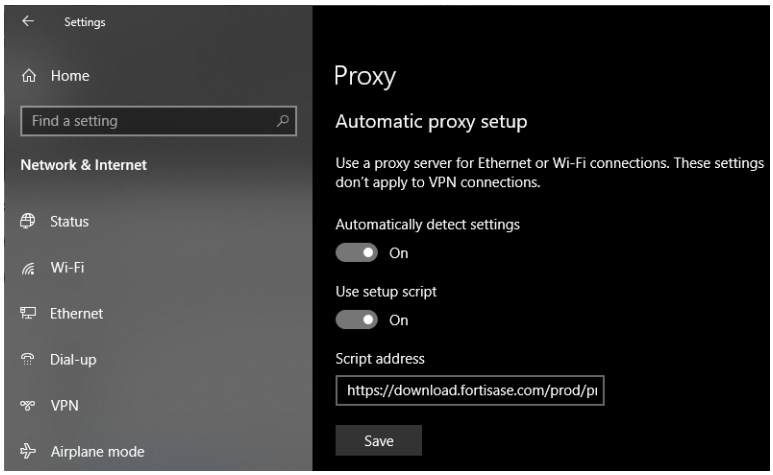
Configuring FortiSASE as an SWG server

The end user follows these instructions to configure SWG agentless mode on their machine. The end user can configure SWG settings at the OS level or in a browser. When SWG settings are configured at the OS level, they are applied to all installed browsers. The following gives instructions for configuring SWG settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE SWG server:

1. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
2. Enable *Use setup script*.

3. In the *Script address* field, enter the *Hosted PAC File* URL.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their Windows domain credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

Configuring FortiSASE with a RADIUS server for remote user authentication

The RADIUS server must be reachable from the public internet.

- If the RADIUS server is behind a firewall, ensure that port 1812 for authentication is open and correctly forwarded. The RADIUS server requires a NAS IP address to be configured in its list of authorized NAS clients. For FortiSASE, this request is done using the public IP address, as listed in Appendix A - FortiSASE data centers on page 324.
- If the RADIUS server is behind a device that can take traffic captures, it is recommended to take a capture to see the RADIUS authentication exchange to see the NAS IP address that FortiSASE uses to make the request.
- If the RADIUS server is a FortiAuthenticator, you must configure the identified NAS IP address as a valid NAS client in the *RADIUS Service* section.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

To configure the RADIUS server in FortiSASE:

1. Go to *Configuration* > *RADIUS*.
2. Click *Create*.

3. Configure the following settings:

Field	Description
Name	Connection name.
Access Type	When set to *Private*, secure private access (SPA) is used for the RADIUS server. Ensure the SPA network is configured.
Authentication Type	If you know the RADIUS server uses a specific authentication protocol, select *Specify* and select the desired protocol from the list. Otherwise, select *Default*.
Include All Users	Allow all users on the RADIUS server to authenticate with FortiSASE.

4. Configure the following *Configure Servers* settings. If the primary server does not respond, FortiSASE sends the access request to the secondary server if configured:

Field	Description
Primary Server	
IP/Name	Enter the domain name or IP address of the RADIUS server.
Secret	Enter the server secret key. This value must match the secret on the RADIUS primary server.
Secondary Server	
IP/Name	(Optional) Enter the domain name or IP address of the secondary RADIUS server.
Secret	(Optional) Enter the secondary server secret key. This value must match the secret on the RADIUS secondary server.

5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the RADIUS server(s), or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

To invite users using RADIUS authentication to FortiSASE:

The following procedure is not applicable for SWG agentless mode users. See SWG agentless mode on page 15.

1. (Optional) If you want to define a group of users, create a user group:
   a. Go to *Configuration* > *Users*.
   b. Click *Create* > *User Group*.
   c. In the *Members* field, click +.
   d. In the *Select Entries* pane, select the desired users to add to this user group.
   e. In the *Remote Groups* field, select *Create*.
   f. From the *Remote Server* dropdown list, select the desired server.
   g. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
   h. Click *OK*.
2. Go to *Dashboards* > *Status*.

3. In the *Remote User Management* widget, click *Onboard Users*.
4. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
5. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Configuring FortiSASE with Entra ID SSO: SAML configuration fields

Before you configure FortiSASE with Microsoft Entra ID single sign on (SSO) for the FortiClient agent-based mode (VPN user SSO) or secure web gateway (SWG) mode (SWG user SSO), review the following tables to understand which Entra ID basic SAML configuration fields correspond to FortiSASE SAML fields.

For the *Configure Identity Provider* step, this table maps the FortiSASE SAML fields that you must copy from FortiSASE and configure in Entra ID:

FortiSASE SAML field	Entra ID Basic SAML configuration field
Entity ID	*Identifier (Entity ID)*
Assertion Consumer Service (ACS) URL	*Reply URL (Assertion Consumer Service URL)*
Single Logout Service (SLS) URL	*Logout Url (Optional)*
Portal (Sign On) URL	*Sign on URL*

Only a single group claim is allowed in the *User Attributes & Claims* section in Entra ID. You will need to delete the existing group claim and then add a new claim, or you can edit the existing group claim. With this approach, the end result is to change *user.groups* to *All groups* with a custom *Claim Name* of *group*.

Alternatively, you can keep the existing group claim with default settings of *user.groups* set to *Security Groups* with *Claim Name* of *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*. This is a valid approach using the official claim name specified by Microsoft.

Regardless of the approach chosen, you must ensure that in the FortiSASE SAML SSO user settings, the *SAML Claims Mapping > Group Name* field matches the *Claim Name* specified in the *User Attributes & Claims* section in the Entra ID SAML settings for the FortiSASE enterprise application.

For the *Configure Service Provider* step, this table maps the Entra ID SAML fields that you must copy from Entra ID and configure in FortiSASE:

FortiSASE SAML field	Entra ID Basic SAML configuration field
IdP Entity ID	Entra ID Identifier
IdP Single Sign-On URL	Login URL
IdP Single Log-Out URL	Logout URL
SAML Claims Mapping > Username	username

FortiSASE SAML field	Entra ID Basic SAML configuration field
SAML Claims Mapping > Group Name	group
SAML Group Matching > Group ID	Object Id (See following steps for identifying this field from a newly created group in Entra ID.)
IdP Certificate	Base64 SAML certificate name (See following steps for downloading this certificate from Entra ID.) The certificate name must be alpanumeric and less than 30 characters.
Service Provider Certificate	You can use the built-in *FortiSASE Default Certificate* or your custom certificate from the dropdown list. To import the certificate click + and import the certificate. See Certificates on page 268.
Digest Method	Use SHA-1 and SHA-256 depending on the hashing method that the IdP supports.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

FortiSASE Default Certificate also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

While configuring *Service Provider Certificate*, the FortiSASE instances that have existing or old SSO configuration, are by default configured with legacy default certificate (i.e. *Fortinet_Factory*) as its service provider certificate.

FortiSASE administrators have an option to change legacy default certificate (i.e. *Fortinet_Factory*) to use new *FortiSASE Default Certificate*. Once FortiSASE is configured to use *FortiSASE Default Certificate*, FortiSASE administrators can no longer configure and use the legacy default certificate (i.e. *Fortinet_Factory*). Thus, ensure to update the service provider certificate in your IdP configuration. Other FortiSASE instances, with fresh SSO configuration have the direct option to use the *FortiSASE Default Certificate* in the *Service Provider Certificate* dropdown menu.

To find the Entra ID group ObjectID in Entra ID:

Enable and configure SAML group matching if you only want to allow Entra ID users of a certain group to authenticate. Otherwise, leave this setting disabled. You can define more granular groups when configuring user group settings.

1. In the left pane of the Azure portal (three horizontal lines), go to *Microsoft Entra ID > Manage > Groups*.
2. The default view shows all groups. Find the desired group and note the *Object Id*.

For details on creating a new security group, see Tutorial: Entra ID SSO Integration with FortiGate SSL VPN.

You can find the full group claims list in Configure group claims for applications by using Microsoft Entra ID.

To download the IdP certificate from Azure:

1. In Entra ID, go to your Entra ID enterprise application, go to *Single sign-on > SAML Signing Certificate*.
2. For *Certificate (Base64)*, click *Download* to download the identity provider certificate to your computer.

Configuring FortiSASE with Entra ID SSO in FortiClient agent-based mode

You can configure a single sign on (SSO) connection with Microsoft Entra ID via SAML, where Entra ID is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to connect to VPN by logging in with their Entra ID credentials.

Before completing the following steps, see Configuring FortiSASE with Entra ID SSO: SAML configuration fields on page 209 for details on how Entra ID SAML fields map to FortiSASE SAML fields.

Configuring FortiSASE with Entra ID SSO

To configure FortiSASE with Entra ID SSO:

1. In FortiSASE, go to *Configuration* > *VPN User SSO*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
   a. In the Azure portal, go to *Microsoft Entra ID* > *Enterprise applications* > *New application*.
   b. Search for and select FortiSASE.
   c. Click *Create*.
   d. Assign Entra ID users and groups to FortiSASE.
   e. Go to *Set up single sign on*.
   f. For the SSO method, select *SAML*.
   g. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.
3. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <FortiSASE instance name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier*, and *Logout URL* fields.
4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL*, and *Logout URL* fields, respectively.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   c. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
   d. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

FortiSASE Default Certificate also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

5. Review the SAML configuration, then click *Submit*.

6. (Optional) If you want Entra ID to perform SP signature verification, download the *Service Provider Certificate* from FortiSASE from *System* > *Certificate*, select *FortiSASE Default Certificate* and click *Download*. On the Azure application, under *SAML Certificates*, upload the FortiSASE Default Certificate and select the digest method that matches to what is configured on FortiSASE in step 4.d.
7. Invite Entra ID users to FortiSASE:
   a. (Optional) If you want to define a group of users, create a user group:
      i. Go to *Configuration* > *Users*.
      ii. Click *Create* > *User Group*.
      iii. In the *Members* field, click +.
      iv. In the *Select Entries* pane, select the desired users to add to this user group.
      v. In the *Remote Groups* field, select *Create*.
      vi. From the *Remote Server* dropdown list, select the desired server.
      vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
      viii. Click *OK*.
   b. In *Configuration* > *Single Sign On (SSO)*, click *Onboard Users*.
   c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
   d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

FortiSASE supports configuring multifactor authentication (MFA) on Entra ID and prompts the user to enter the token code on FortiClient. You must enable and configure MFA on Entra ID for required users. See Enable per-user Microsoft Entra multifactor authentication to secure sign-in events.

Verifying Entra ID SAML SSO configuration

To verify the Azure SAML SSO configuration:

1. In FortiClient on an endpoint, go to the *REMOTE ACCESS* tab. The tab should display a *SAML Login* button.
2. Click the *SAML Login* button.
3. In the dialog, sign in with your Entra ID credentials to connect to VPN.

Configuring API permissions and determining Entra ID SSO credentials

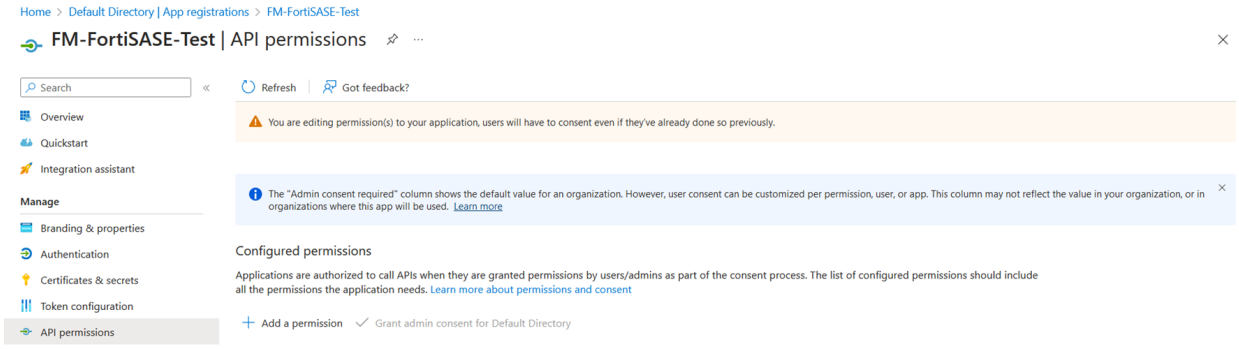
Before you can autoconnect to VPN using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

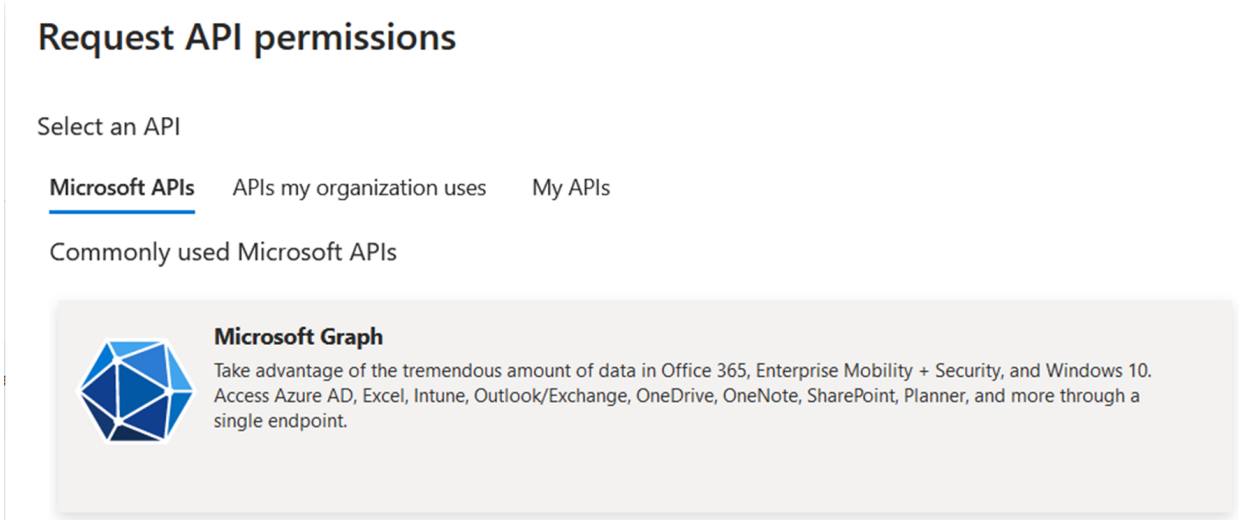
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

To add Microsoft Graph API application permissions required for autoconnect and searching user groups:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.



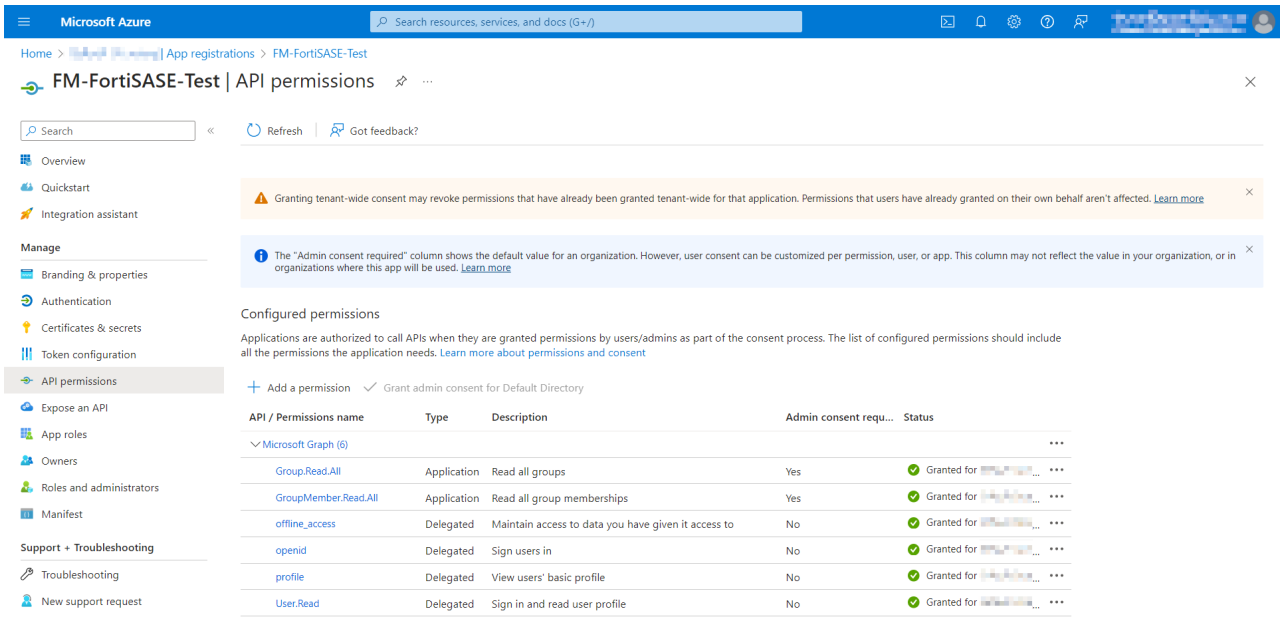
4. In the *Request API permissions* slide-in, click *Microsoft Graph*.



5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*\
   c. Click *Add permissions*.
6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
      - *Openid permissions > offline_access – Maintain access to data you have given it access*
      - *Openid permissions > openid – Sign users in*

- *Openid permissions > profile – View users' basic profile*
- *User > User.Read – Sign in and read user profile*

7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent* confirmation prompt. Observe the *Grant consent successful* notification at the top-right.
   Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.



This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.

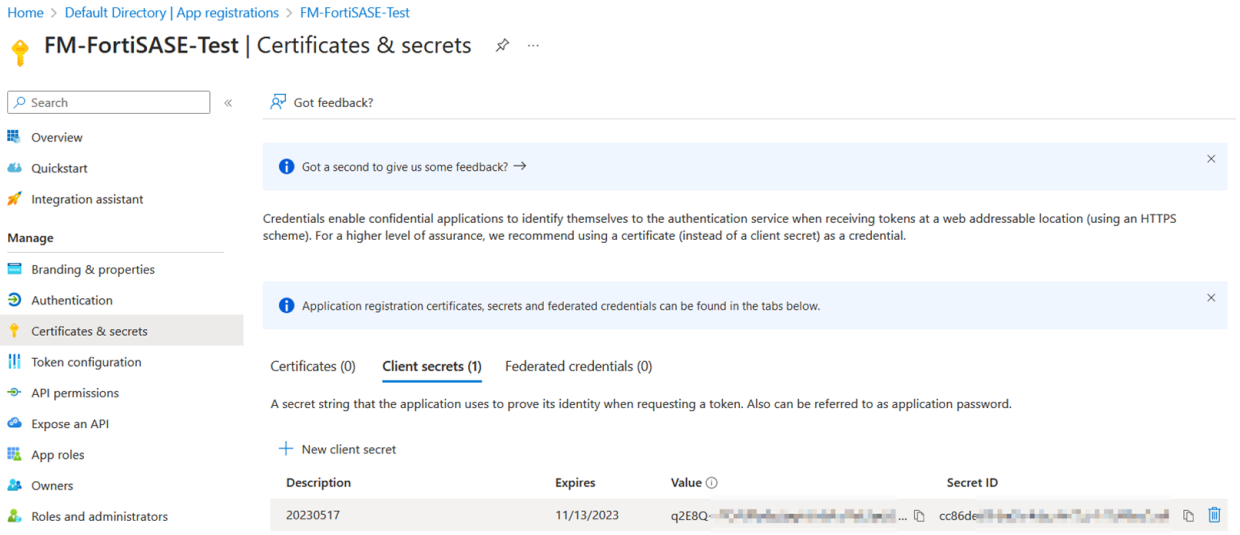
Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

Feature	API permission group	Permission name	Type
VPN autoconnect	*OpenId permissions*	*offline_access*	Delegated
	OpenId permissions	*openid*	
	OpenId permissions	*profile*	
	User	*User.read*	
Group searching	*Group*	*Group.Read.All*	Application
	GroupMember	*GroupMember.Read.All*	

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.

5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

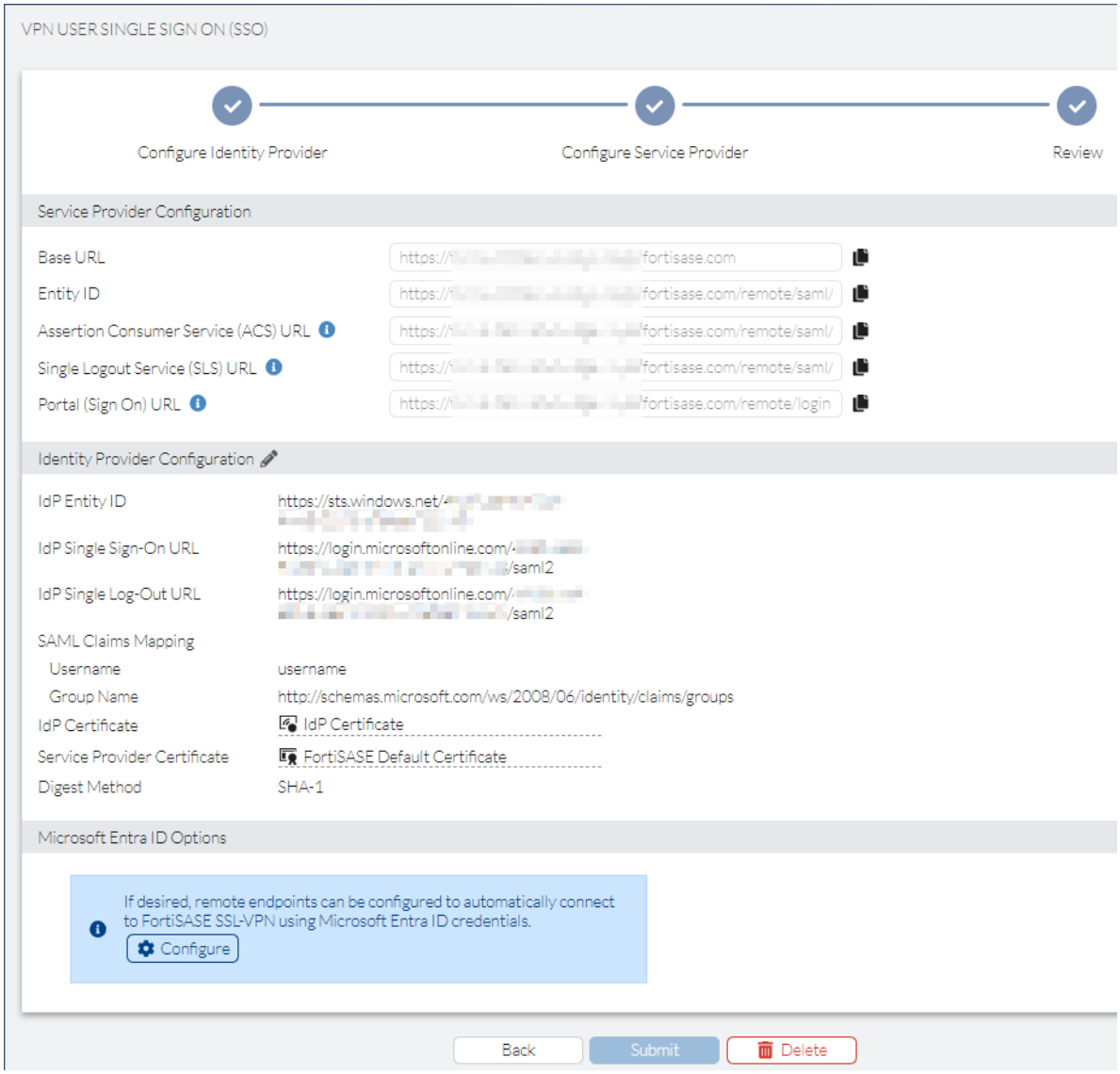
Configuring Entra ID options for agent-based VPN autoconnect

VPN autoconnect is a feature that only the FortiClient agent for Windows supports. Therefore, the *Microsoft Entra ID Options* configuration settings and the FortiSASE agent-based VPN autoconnect using Microsoft Entra ID use case apply to Windows endpoints only.

You must configure FortiSASE with Entra ID options, namely the domain name and application ID, to automatically connect to FortiSASE remote VPN using Entra ID credentials. The FortiSASE Endpoint Management Service uses this information to configure the remote access profile on the FortiClient agent installed on a Windows endpoint. The FortiClient agent for Windows also uses this information to automatically establish a remote VPN connection immediately after FortiClient is installed, and every time a user logs into Windows.

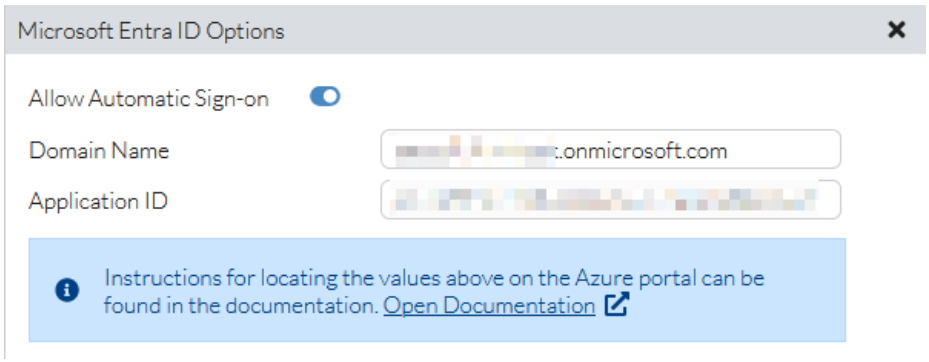
To configure FortiSASE with Entra ID options:

1. In *Configuration* > *VPN User SSO*, ensure that *Service Provider Configuration* and *Identity Provider Configuration* are already configured as Configuring FortiSASE with Entra ID SSO in FortiClient agent-based mode on page 211 describes.
2. Under *Microsoft Entra ID Options*, click *Configure*.



3. In the *Microsoft Entra ID Options* slide-in, select *Allow Automatic Sign-on* and enter the domain name and

application ID.



For instructions for locating the domain name and application ID on the Azure portal and deployment details for configuring remote Windows endpoints with the FortiClient agent for Windows to automatically connect to FortiSASE remote VPN using Entra ID credentials, see the FortiSASE Agent-based VPN Auto-Connect using Entra ID SSO Deployment Guide.

Searching user groups from Entra ID SSO

After performing preliminary steps and determining the Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) single sign on (SSO) credentials, you can proceed to configure them in FortiSASE to allow dynamic group discovery from Entra ID SSO and select a group for SAML group matching.

The following example is for searching user groups from Entra ID SSO from FortiSASE for a FortiClient agent-based mode SSO configuration and demonstrates general steps that also apply to a secure web gateway mode SSO configuration.

To search user groups from Entra ID SSO in FortiClient agent-based mode:

1. Go to *Configuration* > *VPN User SSO*.
   a. For a new configuration, enter the Entra ID SSO fields.
   b. For an existing configuration, click the pencil icon to the right of *Identity Provider Configuration*.
2. Select *SAML Group Matching* and click *Search*.
3. From the *SAML Provider Type* dropdown list, select *Entra ID*. Next to *SAML Provider Credential*, click *Change*.
4. Enter the Entra ID credentials obtained from the Entra ID portal:
   - Tenant ID
   - Client ID
   - Client Secret
5. Click *OK* to save the credentials.
6. Click *Select group* next to *SAML Remote User Groups* and notice that the groups are dynamically obtained from Entra ID and populated. Select a remote user group from the table and click *OK* to save the changes.
7. Notice that the *Configure Service Provider* page has the *Group Name* automatically filled in with the selected user group's name. Click *Next* to advance this page and click *Submit* on the *Review* page to submit the VPN user SSO configuration settings.

Configuring FortiSASE with Entra ID SSO in SWG agentless mode

You can configure a single sign on (SSO) connection with Microsoft Entra ID, where Entra ID is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to configure FortiSASE as their secure web gateway (SWG) server and authenticate using their Entra ID credentials.

Before completing the following steps, see Configuring FortiSASE with Entra ID SSO: SAML configuration fields on page 209 for details on how Entra ID SAML fields map to FortiSASE SAML fields.

Configuring FortiSASE with Entra ID SSO

To configure FortiSASE with Entra ID SSO:

1. In FortiSASE, go to *Configuration* > *SWG User SSO*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
   a. In the Azure portal, go to *Microsoft Entra ID* > *Enterprise applications* > *New application*.
   b. Search for and select FortiSASE.
   c. Click *Create*.
   d. Assign Entra ID users and groups to FortiSASE.
   e. Go to *Set up single sign on*.
   f. For the SSO method, select *SAML*.
   g. In *Basic Configuration*, enter the values that you copied in step 1 in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.
3. Obtain the IdP information from Azure:
   a. The *SAML Signing Certificate* box contains links to download the SAML certificate. Download the certificate.
   b. The *Set up <FortiSASE instance name>* box lists the IdP information that you must provide to FortiSASE. Copy the values in the *Login URL*, *Entra ID Identifier*, and *Logout URL* fields.
4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *Entra ID Identifier*, *Login URL*, and *Logout URL* fields, respectively.
   b. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   c. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
   d. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

   FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

   FortiSASE Default Certificate also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.
5. Review the SAML configuration, then click *Submit*.

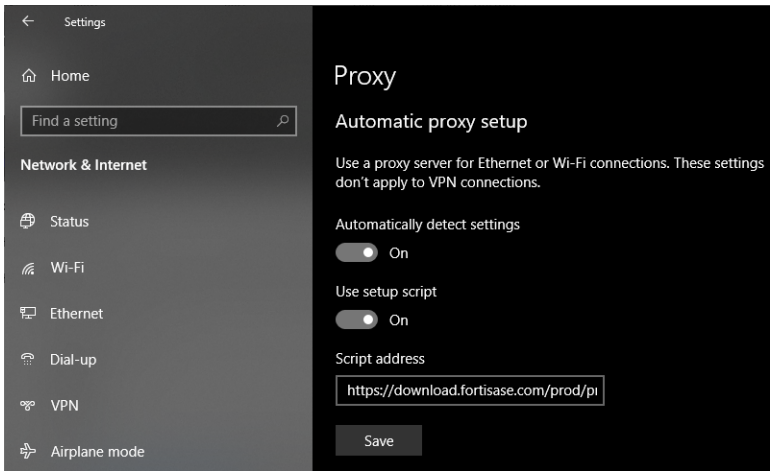
6. (Optional) If you want Entra ID to perform SP signature verification, download the *Service Provider Certificate* from FortiSASE from *System* > *Certificate*, select *FortiSASE Default Certificate* and click *Download*. On the Azure application, under *SAML Certificates*, upload the FortiSASE Default Certificate and select the digest method that matches to what is configured on FortiSASE in step 4.d.

Configuring FortiSASE as a SWG server

The end user follows these instructions to configure SWG agentless mode on their machine. The end user can configure SWG settings at the OS level or in a browser. When the user configures SWG settings at the OS level, they are applied to all installed browsers. The following gives instructions for configuring SWG settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE SWG server:

1. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
2. Enable *Use setup script*.
3. In the *Script address* field, enter the *Hosted PAC File* URL.



4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their Entra ID credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

Configuring FortiSASE with AD FS SSO

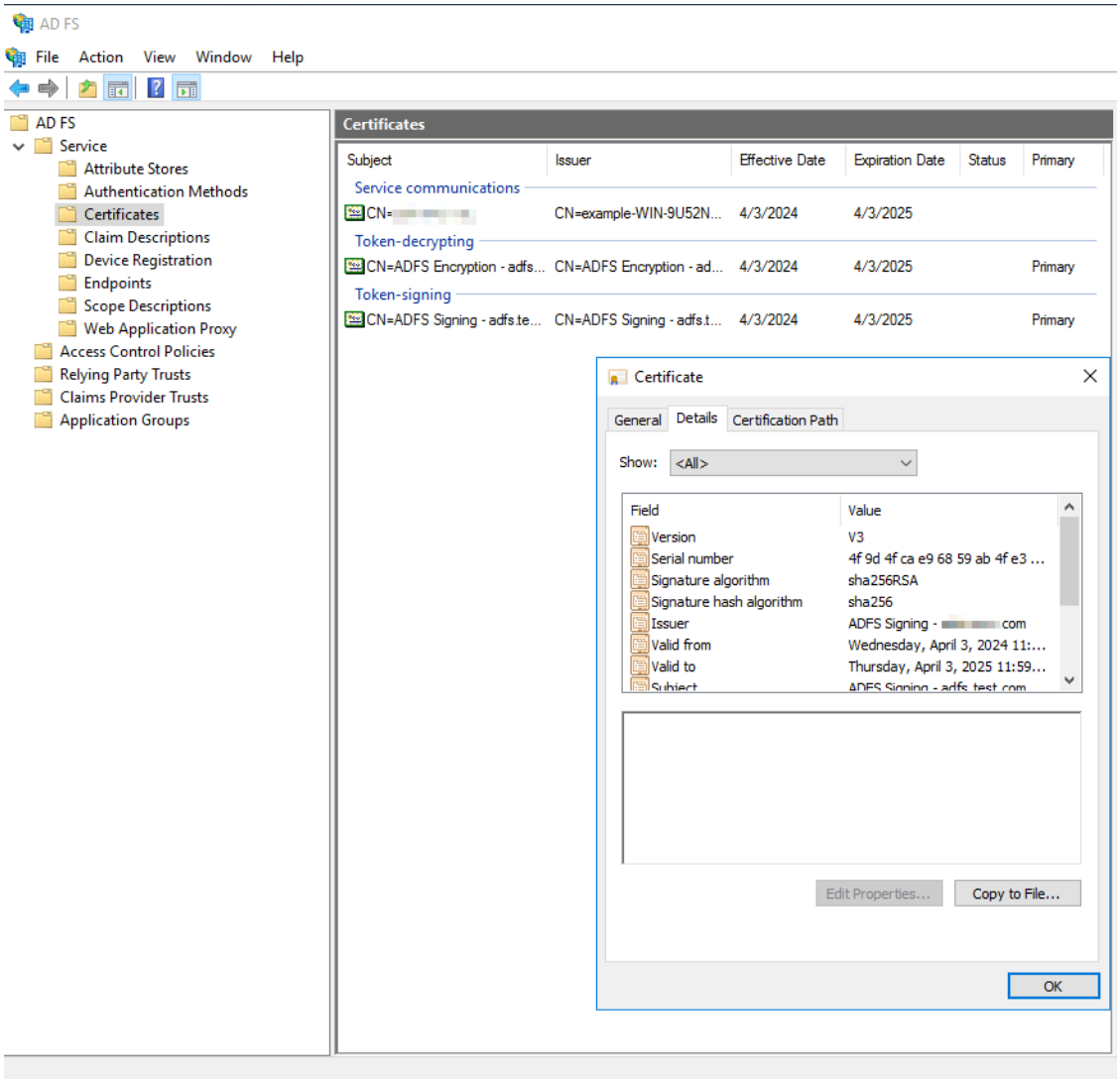
FortiSASE supports claims-based SAML user authentication using Active Directory Federation Services (AD FS). FortiSASE acts as a service provider (SP) and AD FS acts as an identity provider (IdP) in the SAML authentication flow. In AD FS terminology, FortiSASE is also called a relying party.

The example that this topic discusses assumes that you have completed prerequisites to install AD FS, and the AD FS service is already installed on Windows Server 2016. See AD FS Requirements.

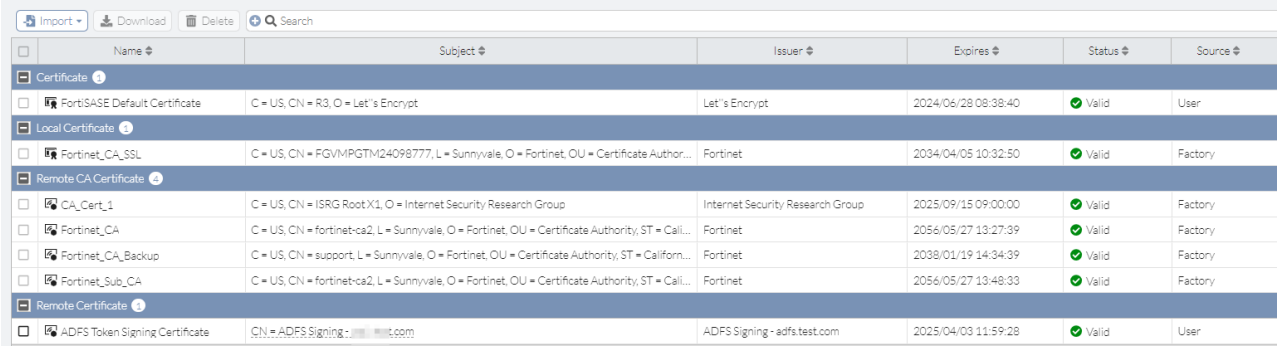
To export an IdP certificate from AD FS and import it in FortiSASE:

1. On Windows 2016 Server Manager, open the AD FS management snap-in from *Server Manager* > *Tools* > *AD FS Management*.

2. From the *Service* dropdown list, select *Certificates*. Double-click the certificate under *Token-signing*. In the *Certificate* menu, go to the *Details* tab and select *Copy to File* to export it to a suitable location using either .CER format.



3. To import this certificate to FortiSASE, move it to a location that the machine where you will open the FortiSASE GUI can access.
4. In FortiSASE, go to *System* > *Certificates*. *Select Import* > *Remote Certificate*. For *Type*, select *Remote Certificate* and click *Upload* to import the IdP certificate. Give a suitable *Certificate Name* as desired.
5. Click *OK*. The certificate is visible under *System* > *Certificates* > *Remote Certificate*. In this example, FortiSASE successfully imported *ADFS Token Signing Certificate*.



To export an SP certificate from FortiSASE:

In FortiSASE, go to *System* > *Certificate*, click *FortiSASE Default Certificate* and click *Download* from the toolbar. You will import this certificate to AD FS as the SP certificate in To configure AD FS relying party trust: on page 222.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

FortiSASE Default Certificate also periodically renews. Thus, if IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

To retrieve IdP Configuration from AD FS:

1. On the Windows server where AD FS is installed, open a web-browser to download the Federation metadata XML file using the URL https://<your-adfs.domain.com>/federationmetadata/2007-06/FederationMetadata.xml>, where your-adfs.domain.com is the FDQN of your AD FS server.
2. Open the XML file and search for *entityID*, *SingleSignOnService Location*, and *SingleLogoutService Location* and copy the values (i.e. URLs) for these fields in a notepad file:

   ```
   entityID="http://<your-adfs.domain.com>/adfs/services/trust"
   ```

   ```
   <SingleSignOnServiceLocation="https://<your-adfs.domain.com>/adfs/ls/"
   ```

   ```
   <SingleLogoutServiceLocation="https://<your-adfs.domain.com>/adfs/ls/"
   ```

   These URLs will be used to configure IdP details on FortiSASE in To configure AD FS SSO on FortiSASE: on page 221.

To configure AD FS SSO on FortiSASE:

1. In FortiSASE, to configure SSO for agent-based users, go to *Configuration* > *VPN User SSO*. Similarly, for agentless users using FortiSASE SWG, go to *Configuration* > *SWG User SSO*.
2. For *Configure Identity Provider*, copy the values in the *Entity ID*, *Assertion Consumer Service (ACS) URL*, and *Single Logout Service (SLS) URL* fields to a Notepad file. These URLs are used in To configure AD FS relying party trust: on page 222. Click *Next*.
3. In *Configure Service Provider*, paste the values (i.e. URLs) from Notepad that you retrieved in To retrieve IdP Configuration from AD FS: on page 221 with the following mapping:

FortiSASE	Values copied from AD FS
IdP Entity ID	http://<your-adfs.domain.com>/adfs/services/trust
IdP Single Sign-On URL	https://<your-adfs.domain.com>/adfs/ls/
IdP Single Log-Out URL	https://<your-adfs.domain.com>/adfs/ls/

4. For *SAML Claims Mapping*, in the FortiSASE *Username* field, enter username as copied from AD FS.
5. Disable *SAML Group Matching*.
6. From the dropdown list, select the IdP certificate that was imported into FortiSASE in To export an IdP certificate from AD FS and import it in FortiSASE: on page 219:
7. For *Service Provider Certificate*, select *FortiSASE Default Certificate*.

While configuring *Service Provider Certificate*, the FortiSASE instances that have existing or old SSO configuration, are by default configured with legacy default certificate (i.e. *Fortinet_Factory*) as its service provider certificate.

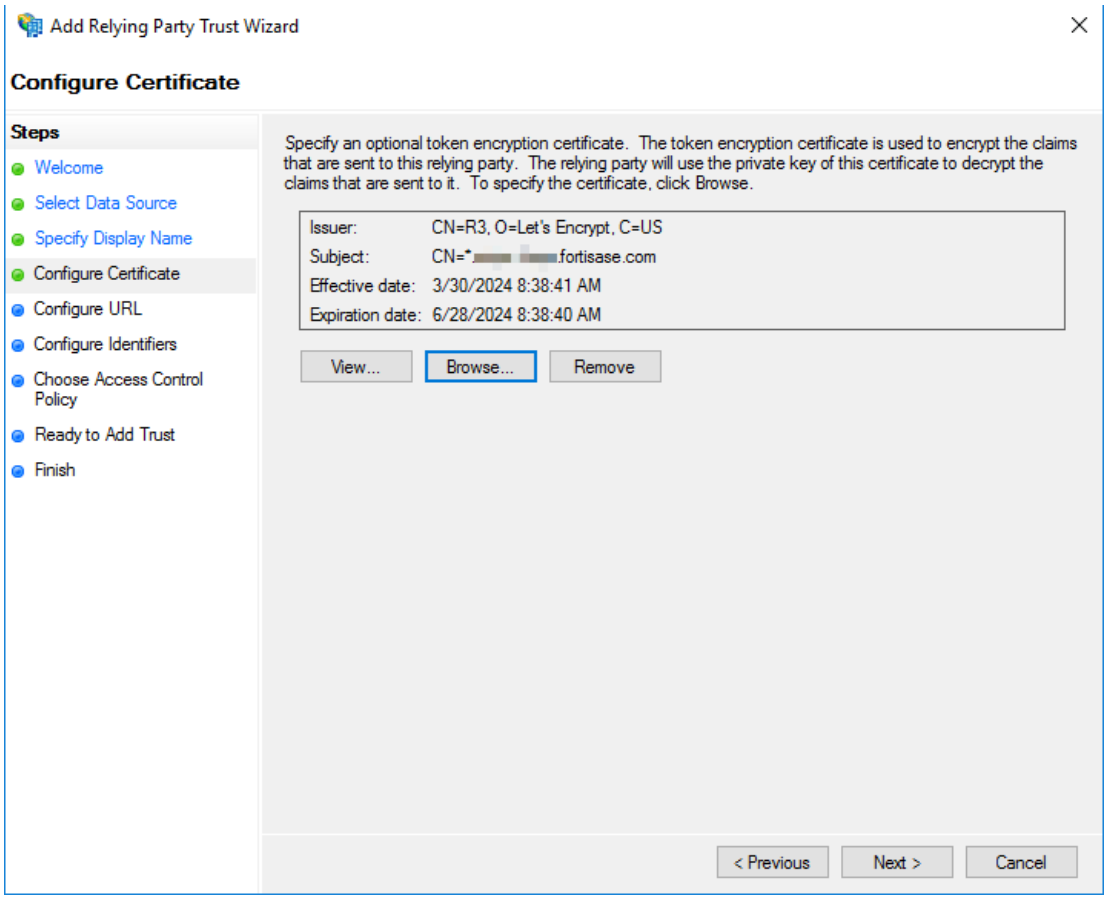
FortiSASE administrators have an option to change legacy default certificate (i.e. *Fortinet_Factory*) to use new *FortiSASE Default Certificate*. Once FortiSASE is configured to use *FortiSASE Default Certificate*, FortiSASE administrators can no longer configure and use the legacy default certificate (i.e. *Fortinet_Factory*). Thus, ensure to update the service provider certificate in your IdP configuration. Other FortiSASE instances, with fresh SSO configuration have the direct option to use the *FortiSASE Default Certificate* in the *Service Provider Certificate* dropdown menu.

The *FortiSASE Default Certificate* also periodically renewed. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

8. For *Digest Method*, select *SHA-256*. FortiSASE supports both SHA-1 and SHA-256, but AD FS is by default configured with SHA-256 and this hash algorithm is also recommended by Microsoft.
9. Click *Next* and then click *Submit*. Click *OK* after reading the Caution prompt.

To configure AD FS relying party trust:

1. On Windows Server, open the *AD FS Management* snap in.
2. Right-click *Relying Party Trust* and select *Add Relying Party Trust*.
3. In the *Welcome* step, select *Claims aware*, then *Start*.
4. In the *Select Data Source* step, select *Enter data about the relying party manually*. Click *Next*.
5. In the *Specify Display Name* step, give the relying party a suitable *Display name* (such as SASE). Click *Next*.
6. (Optional) To encrypt the token claims sent to the relying party (i.e. FortiSASE), in the *Configure Certificate* step, copy the certificate *FortiSASE Default Certificate* downloaded in To export an SP certificate from FortiSASE: on page 221 and move it to Windows Server in a suitable directory. Upload the certificate by clicking *Browse* to navigate to directory. Click *Next*.

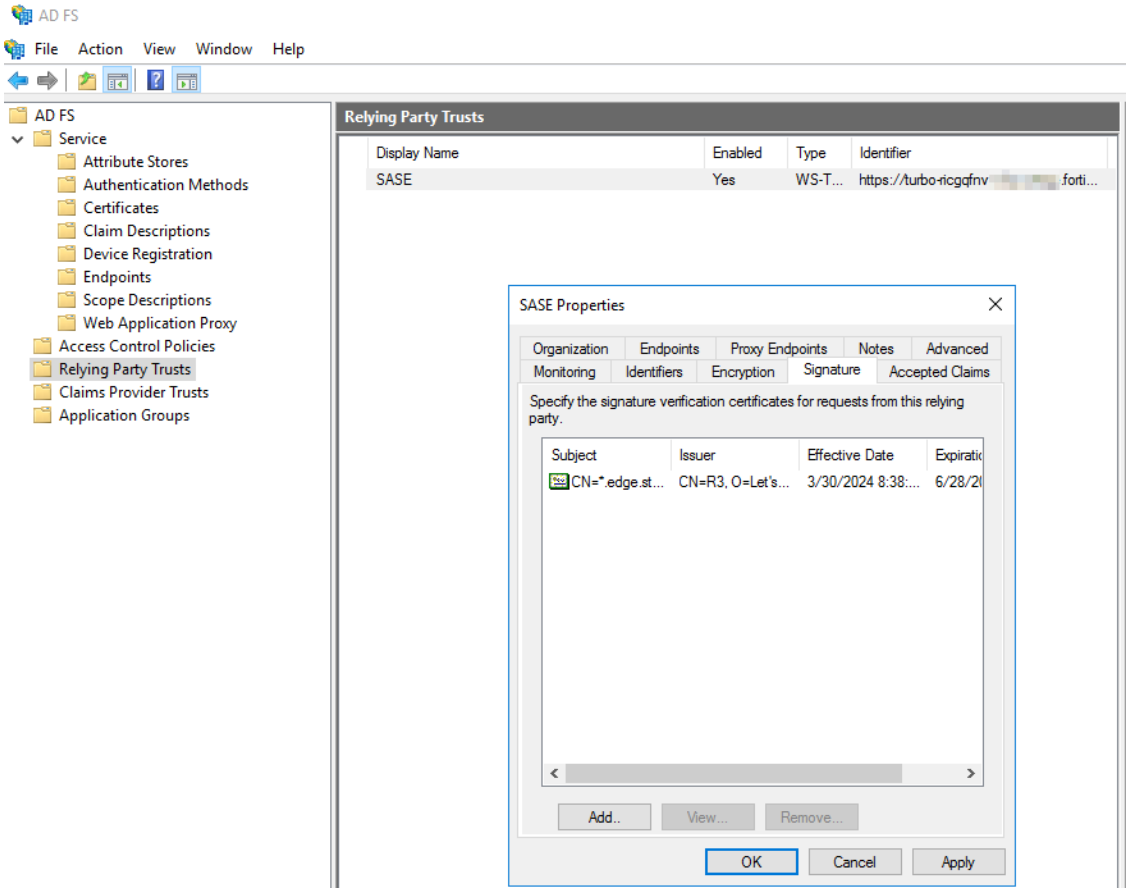


7. In the *Configure URL* step, select *Enable support for the SAML 2.0 WebSSO protocol* and enter the *Assertion Consumer Service (ACS) URL* from To configure AD FS SSO on FortiSASE: on page 221. Click *Next*.
8. In the *Configure Identifiers* step, in the *Relying party trust identifier* field, paste the *Entity ID* value from To configure AD FS SSO on FortiSASE: on page 221. Click *Add*, then *Next*.
9. In the *Choose Access Control Policy* step, *Permit everyone* is selected by default. If desired, restrict the access control policy to a specific group. Click *Next*. In the *Ready to Add Trust* step, click *Next*. In the *Finish* step, click *Close*.

To configure properties of AD FS Relying Party Trusts.

1. On the *AD FS* management snap-in, click *Relying Party Trusts*. Right-click your configured relying party trust and click *Properties*.
2. On the *Signature* tab, click *Add* to go to the folder to add *FortiSASE Default Certificate*.

3. Click *Apply*.

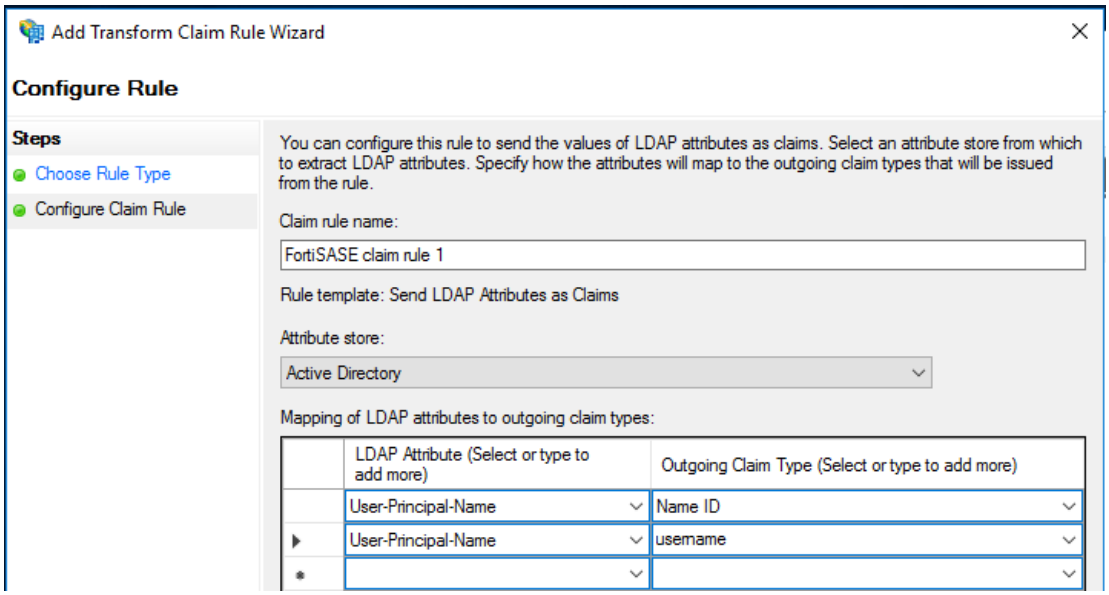


4. On the *Advanced* tab, for *Secure hash algorithm*, select *SHA-256*.
5. Click *OK*.

To configure AD FS Claim Issuance Policy

1. On the *AD FS* management snap-in, click *Relying Party Trusts*. Right-click your configured relying party trust and click *Edit Claim Issuance Policy*.
2. In *Issuance Transform Rules*, click *Add Rule*. A new *Add Transform Claim Rule Wizard* opens.
3. For *Choose Rule Type*, in the *Claim rule template*, select *Send LDAP Attributes as Claims* from the dropdown list. Click *Next*.
4. In *Configure Claim Rule*, give a suitable claim rule name.
5. For *Attribute store*, select *Active Directory*.
6. Enter the following claims that FortiSASE supports:

LDAP Attribute	Outgoing Claim Type
User-Principal-Name	Select *Name ID* from the dropdown list.
User-Principal-Name	username. As username is not available to select from the dropdown list, you must enter it manually.



7. Click *Finish*. The claim rule is visible under *Claim Issuance Policy*.
8. Click *Apply*. Click *OK*.

To configure SAML user groups on FortiSASE:

1. On FortiSASE, go to *Configuration* > *Users & Groups*.
2. Click *Create*, select *User Group*.
3. Click *Next*.
4. Enter a suitable *Name* for the group. From the *Remote Groups* table, click *Create*.
5. From the *Remote Server* dropdown list, select *VPN SSO*. You must select *VPN SSO* even if you are using SWG.
6. Click *OK* to save the remote server configuration.
7. Click *OK* to save the user group configuration.
8. Use the user group created inside respective policies for agent-based users or secure web gateway policies for agentless users to authenticate users connecting to FortiSASE using SSO using AD FS. See Policies on page 139 and SWG Policies on page 142.
9. For agentless users, do the following:
   a. Download the PAC file from *System* > *SWG configuration*. See Downloading the preconfigured PAC file on page 287.
   b. Customize the PAC file to add IdP URLs to exempt the IdP traffic to flow through FortiSASE. See Customizing the PAC file on page 287.
   c. Configure the proxy setting on your endpoint using the customized PAC file. See Windows on page 292.

While setting up SSO with AD FS or other custom identity providers (IdP) (except Google, Entra ID, FortiTrustID, or Okta) for agentless users, customizing the PAC file to add IdP URLs to it such that the traffic to IdP URLs is not forwarded to the FortiSASE secure web gateway (SWG) server and instead goes directly to the internet is mandatory. See Customizing the PAC file on page 287.

Configuring FortiSASE with Okta SSO

You can configure a single sign on (SSO) connection with Okta via SAML, where Okta is the identity provider (IdP) and FortiSASE is the service provider (SP). This feature allows end users to connect to VPN by logging in with their Okta credentials.

To configure FortiSASE with Okta SSO:

1. In FortiSASE, go to *Configuration* > *VPN User SSO*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Okta. Copy these values.
2. Create and configure your FortiSASE environment in Okta:
   a. Add the FortiSASE application to Okta:
      i. On the Okta administration page, go to *Applications*.
      ii. Click *Add Application*.
      iii. In the searchbox, search for and select FortiSASE.
      iv. Click *Add*.
      v. Under *General Settings*, click *Done*.
   b. On the *Assignment* tab, from the *Assign* dropdown list, select *Assign to People*.
   c. In the dialog, assign the desired users to the FortiSASE Okta application.
   d. On the *Sign On* tab, click *Edit*.
   e. Paste the entity ID value from FortiSASE in the *Base URL* field in Okta. After pasting, edit this value to remove everything after the URL,"fortisase.com".
   f. Click *Save*.
3. Obtain the IdP information from Okta:
   a. On the *Sign On* tab in Okta, click *View Setup Instructions*.
   b. Scroll to step 5. This step lists the IdP information that you must provide to FortiSASE. Copy the values in the *IdP Entity ID*, *IdP Single Sign-On URL*, and *IdP Single Log-Out URL* fields.
   c. Download the IdP certificate from the provided link. Save the certificate to your device.
4. Configure the IdP information in FortiSASE:
   a. In FortiSASE, click *Next* in the SSO wizard. In the *IdP Entity ID*, *IdP Single Sign-On URL*, *IdP Single Log-Out URL* fields, paste the values that you copied from the *IdP Entity ID*, *IdP Single Sign-On URL*, and *IdP Single Log-Out URL* fields, respectively.
   b. In *SAML Claims Mapping*, in the *Username* field, enter username. In the *Group Name* field, enter group. Both fields are case-sensitive. If you have configured to use SAML attribute names other than username or group on Okta, you can enter the SAML attribute name in the *Username* and *Group Name* fields accordingly.
   c. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
   d. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
   e. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

FortiSASE Default Certificate also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.

5. Review the SAML configuration, then click *Submit*.
6. Invite Okta users to FortiSASE:
   a. (Optional) If you want to define a group of users, create a user group:
      i. Go to *Configuration* > *Users*.
      ii. Click *Create* > *User Group*.
      iii. In the *Members* field, click +.
      iv. In the *Select Entries* pane, select the desired users to add to this user group.
      v. In the *Remote Groups* field, select *Create*.
      vi. From the *Remote Server* dropdown list, select the desired server.
      vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
      viii. Click *OK*.
   b. In *Configuration* > *Single Sign On (SSO)*, click *Onboard Users*.
   c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
   d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Configuring FortiSASE with FortiTrust ID as SAML IdP proxy for Entra ID SSO

FortiTrust Identity (FortiTrust ID) performs the function of a SAML identity provider (IdP) as well as an IdP proxy and enforces multifactor authentication (MFA). FortiTrust ID is composed of FortiAuthenticator Cloud for IdP and IdP proxy functionality and FortiToken Cloud for MFA including adaptive authentication.

A use case for IdP proxy is when using multiple IdPs to authenticate different user types. For example, you may authenticate employees using Microsoft Entra ID while contractors use Google Workspace or Okta.

You can configure a single sign on (SSO) connection with FortiAuthenticator Cloud via SAML, where FortiAuthenticator Cloud is the IdP, namely, an IdP proxy, and FortiSASE is the service provider (SP). This feature allows end users to connect to VPN by logging in with their corresponding IdP credentials.

This example describes how to set up FortiTrust ID using FortiAuthenticator Cloud as a SAML IdP proxy for Entra ID.

These steps require FortiTrust ID to be running FortiAuthenticator Cloud 6.5.0 or later to support the following features to help with compatibility with third-party IdPs:

- **Sends username in this parameter**: specify the parameter name in which the remote IdP receives the username so as to prefill the username login field.
- **Strip realm from username before sending.**

To upgrade to FortiAuthenticator Cloud 6.5.0 or later, which supports these features, you must send a request to fortitrustid-support@fortinet.com. See the FortiTrust ID Release Notes corresponding to your version, specifically, the *Upgrade Information* section.

1. In the Azure portal, do the following:
   a. Create an enterprise application using FortiSASE as a template from the Azure App Gallery and copy its application ID. See To create an enterprise application using FortiSASE as a template from the gallery and find the application ID of the FortiSASE enterprise application: on page 228.
   b. Register the enterprise application with Microsoft identity platform and generate an authentication key. See To register the enterprise application: on page 229.
   c. Add the enterprise application as an assignment. See To add the enterprise application as an assignment: on page 229.
2. In FortiAuthenticator Cloud, do the following:
   a. Create a remote OAuth server with Azure application ID and authentication key. See To create a remote OAuth server: on page 229.
   b. Start to create a remote SAML server. See To partially configure the remote SAML server on FortiAuthenticator Cloud: on page 229.
3. In the Azure portal, configure SAML settings for the FortiSASE application in Azure. See To configure SAML settings for the FortiSASE application in Azure: on page 230 and To collect SAML IdP URL information: on page 230.
4. In FortiAuthenticator Cloud, do the following:
   a. Continue to create a remote SAML server. See To fully configure the remote SAML server on FortiAuthenticator Cloud: on page 230.
   b. Create a realm for domain name. See To create an Azure realm and add it to the IdP: on page 231.
   c. Enable SAML IdP portal. See To enable the SAML IdP portal: on page 231.
   d. Download IdP certificate. See To download the IdP certificate: on page 231.
   e. Start to create a SAML Service Provider (SP) entry for FortiSASE. See To partially configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud: on page 231.
5. In FortiSASE, configure FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode. See Configuring FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode on page 232.
6. In FortiAuthenticator Cloud, continue to create a SAML SP entry for FortiSASE. See Configuring FortiAuthenticator Cloud - III on page 233.

Configuring Entra ID

Create a new Entra enterprise application using the FortiSASE application as a template from the Entra app gallery, configure your Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) environment with users and groups and configure the enterprise application for SAML single sign-on (SSO) for the agent-based deployment.

To create an enterprise application using FortiSASE as a template from the gallery and find the application ID of the FortiSASE enterprise application:

1. Log into the Azure portal.
2. Go to *Microsoft Entra ID* > *Enterprise applications* > *New application*.
3. Search for and select *FortiSASE*.
4. Click *Create*.
5. In *Overview* > *Properties*, copy the application ID. You need this information in a later step.
6. Assign Entra ID users and groups to FortiSASE.

To register the enterprise application:

1. Log into the Azure portal.
2. Go to the directory home, and select *App registrations*.
3. In the *App registrations* window, select *All applications*, and search your application by name.
4. In the list, select your application.
5. Go to *Manage* > *Certificates & secrets*, and select + *New client secret*.
6. In the *Add a client secret window*, do the following:
   a. In the *Description* field, enter a description for the client secret.
   b. From the *Expires* dropdown list, select a time period after which the client secret expires.
   c. Select *Add*.

In *Client secrets*, make note of the *Value*.

Since this key is visible only once (immediately after creation), you must recreate the key if you do not copy and store it.

Setting up an OAuth server requires the key.

To add the enterprise application as an assignment:

1. Go to the Microsoft Entra ID directory home, and select *Roles and administrators*.
2. From the *Administrative roles* list, select *Directory readers*.
3. Select the ellipsis for *Directory readers*, then select *Description*.
4. Go to *Assignments* and select *Add assignment*.
5. In the *Add assignments* window, search your application by name, and select *Add*.

Configuring FortiAuthenticator Cloud - I

To create a remote OAuth server:

1. In FortiAuthenticator Cloud, Go to *Authentication* > *Remote Auth. Servers* > *OAUTH* and select *Create New*.
2. Enter a name for the remote OAuth server.
3. In the *OAuth source* dropdown list, select *Azure Directory*.
4. In the *Client ID* field, enter the Entra enterprise application ID that you saved previously.
5. In the *Client Key* field, enter the Client secrets *Value* created previously.
6. Select *OK* to add the remote OAuth server.

To partially configure the remote SAML server on FortiAuthenticator Cloud:

1. In FortiAuthenticator Cloud, go to *Authentication* > *Remote Auth. Servers* > *SAML*, and click *Create New*. In the *Create New Remote SAML Server* page, configure the following:
   a. Select *Proxy* as the *Type*.
   b. For the *Entity ID*, click the dropdown menu and select the Azure identity provider (IdP) option.
   c. Under *Single Logout*, ensure *Enable SAML single logout* is checked.
   d. Copy these SAML fields:
      - Portal URL
      - Entity ID

- ACS (login) URL
- SLS (logout) URL

2. Keep this page open in your web browser since you will continue configuring it after configuring Entra ID.

Configuring SAML settings for the FortiSASE application in Azure

To configure SAML settings for the FortiSASE application in Azure:

1. Log into the Azure portal.
2. Go to *Microsoft Entra ID* > *Enterprise applications*.
3. Select the enterprise application you created previously.
4. Go to *Set up single sign on*.
5. For the *SSO method*, select *SAML*.
6. In *Basic SAML Configuration*, enter the values that you copied in the FortiAuthenticator Cloud Remote *SAML Server* in these fields:

Microsoft Entra ID > Basic SAML Configuration	FortiAuthenticator Cloud > Edit Remote SAML Server
Identifier (Entity ID)	Entity ID
Reply URL (ACS URL)	ACS (login) URL
Sign on URL	Portal URL
Logout URL	SLS (logout) URL

7. Click *Save* and click *X* to close the window.

To collect SAML IdP URL information:

While still in the SAML-based Sign-on page for the enterprise application you created, in the SAML certificates box, do the following:

1. Download the Certificate (Base64) by clicking *Download* and selecting a file location for downloading the certificate file.
2. Download the Federation Metadata XML by clicking *Download* and selecting a file location for downloading the XML file.

Configuring FortiAuthenticator Cloud - II

To fully configure the remote SAML server on FortiAuthenticator Cloud:

1. Go to the open web browser and continue configuring *Create New Remote SAML Server* in FortiAuthenticator Cloud.
2. Confirm *Type* is still set to *Proxy*.
3. For the *Entity ID*, ensure the Azure identity provider (IdP) option is still selected.
4. Since by this point you have already completed the Entra ID SAML configuration and obtained the IdP metadata file, under *IdP Metadata*, click *Import IdP metadata*, select the Federation Metadata XML file saved previously, and click *OK* to import the file. After importing the XML file, observe that the *IdP entity ID* and *IdP single sign-on URL* fields have been populated accordingly.

5. For *Send username in this parameter*, enter *login_hint*.
6. Ensure *Strip realm from username before sending* is unchecked.
7. In *Single logout*, confirm *Enable SAML single logout* is still checked.
8. In *Group Membership*, select *Cloud* and choose the previously created Azure OAuth server. Update the *Groups* field to match what is configured on the Azure side.
9. Click *OK* to save changes.

To create an Azure realm and add it to the IdP:

1. In FortiAuthenticator Cloud, go to *Authentication* > *User Management* > *Realms*.
2. Click *Create New*.
3. Enter the realm name. This should be the domain of the SAML usernames. For example, for usernames such as jsmith@domain.com, the realm name should be set as domain.com.
4. Select the *User source* as the newly created remote SAML authentication server.
5. Click *OK*.

To enable the SAML IdP portal:

1. In FortiAuthenticator Cloud, go to *Authentication* > *SAML IdP* > *General*.
2. Enable *SAML identity provider portal*, and enter the following:
   a. *Username input format*: *username@realm (default)*
   b. *Realms*: click *Add a realm* to add the realm associated with the remote server for Azure IdP.
   c. *Default IdP certificate*: select a default certificate to use.
3. Ensure *Legacy login sequence* is disabled.
4. Click *OK* to save changes.

To download the IdP certificate:

1. In FortiAuthenticator Cloud, go to *Certificate Management* > *End Entities* > *Local Services*.
2. Click *Export Certificate* to export the certificate being used as the *Default IdP certificate*.
3. In the file browser, choose where to save the file and click *Save*.

To partially configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud:

1. In FortiAuthenticator Cloud, go to *Authentication* > *SAML IdP* > *Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
2. Enter the following information:
   a. *SP name*: enter a name for the service provider (SP) device.
   b. *IdP prefix*: select +, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
   c. *Server certificate*: select the same certificate as the default IdP certificate used in *Authentication* > *SAML IdP* > *General*. See Configuring SAML IdP settings.
3. Copy the following information to use for configuring FortiSASE later:
   - IdP entity id
   - IdP single sign-on URL
   - IdP single logout URL
4. Click *Save*.
5. Keep this page open in your web browser since you will continue configuring it after configuring FortiSASE.

Configuring FortiSASE with FortiAuthenticator Cloud in FortiClient agent-based mode

To configure the FortiAuthenticator Cloud IdP information in FortiSASE:

1. In FortiSASE, go to *Configuration* > *VPN User SSO*.
2. Copy the following fields from the *Configure Identity Provider* page. You use these fields to complete the FortiAuthenticator Cloud SAML service provider configuration.
   - Entity ID
   - ACS URL
   - SLS URL
3. Click *Next* in the single sign on (SSO) wizard.
4. In the *IdP Entity ID*, *IdP Single Sign-On URL*, and *IdP Single Log-Out URL* fields, paste the corresponding values that you copied from the FortiAuthenticator Cloud *SAML IdP* > *Service Providers* fields.
5. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded from FortiAuthenticator Cloud. Click *Next*.
6. In the *Service Provider Certificate* field, use *FortiSASE Default Certificate* or your own custom certificate. Click + to add your own custom certificate.
7. For *Digest Method*, select *SHA-1* or *SHA-256*. The digest method should match the digest method on Azure if *Certificate Verification* is enabled on Azure.

   FortiSASE Default Certificate is a built-in wildcard certificate on FortiSASE signed by a well-known public CA and remains same across all of your points of presence.

   FortiSASE Default Certificate also periodically renews. Thus, if the IdPs are using *Service Provider Certificate* in their configuration, administrators must periodically update their IdP configuration with new SP certificate. To avoid having to update your IdP configuration frequently, we recommend uploading your own certificate.
8. Review the SAML configuration, then click *Submit*.
9. Click *OK* to confirm that SSO authentication will take priority over existing LDAP and RADIUS authentication methods.
10. Invite Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) users to FortiSASE:
    a. (Optional) If you want to define a group of users, create a user group:
       i. Go to *Configuration* > *Users*.
       ii. Click *Create* > *User Group*.
       iii. In the *Members* field, click +.
       iv. In the *Select Entries* pane, select the desired users to add to this user group.
       v. In the *Remote Groups* field, select *Create*.
       vi. From the *Remote Server* dropdown list, select the desired server.
       vii. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
       viii. Click *OK*.
    b. In *Configuration* > *Single Sign On (SSO)*, click *Onboard Users*.
    c. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
    d. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

Configuring FortiAuthenticator Cloud - III

To fully configure a SAML SP entry for FortiSASE in FortiAuthenticator Cloud:

1. Go to the open web browser and continue configuring *Edit SAML Service Provider* in FortiAuthenticator Cloud.
2. In the *SP Metadata* pane, enter the SP information from FortiSASE, which you will use as the SAML SP:

FortiSASE > Configuration > VPN User SSO	FortiAuthenticator Cloud > Edit SAML Service Provider
Entity ID	SP entity ID
ACS URL	SP ACS (login) URL
SLS URL	SP SLS (logout) URL

3. In *Assertion Attribute Configuration*, configure the following:
   a. Select *Username* from the *Subject NameID* dropdown list.
   b. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.
4. In *Assertion Attributes*, select *Add Assertion Attribute* and add the following attributes:
   a. SAML attribute: *username*
      User attribute: SAML username
   b. SAML attribute: *groups*
      User attribute: SAML group membership
5. Click *OK* to save changes.

Searching user groups from SAML IdP

From FortiSASE, it is possible to search the user groups on the remote SAML provider configured for VPN and secure web gateway (SWG) SSO by configuring SAML provider credentials in the *Search User Groups from SAML Provider* slide-in window. You can then configure the user groups for SAML group matching. Dynamically discovering a user group from the SAML identity provider (IdP) is more convenient than manually finding a user group's identifier (ID) from the remote SAML provider's portal and configuring it for SAML group matching.

Before you can configure the SAML provider credentials, you must perform some setup and obtain these credentials from the SAML IdP.

Currently, searching user groups from a SAML provider from FortiSASE is supported with Entra ID SSO in FortiClient agent-based mode via *Configuration* > *VPN User SSO*, or in SWG agentless mode via *Configuration* > *SWG User SSO*. See Configuring API permissions and determining Entra ID SSO credentials on page 233 and Searching user groups from Entra ID SSO on page 236.

Configuring API permissions and determining Entra ID SSO credentials

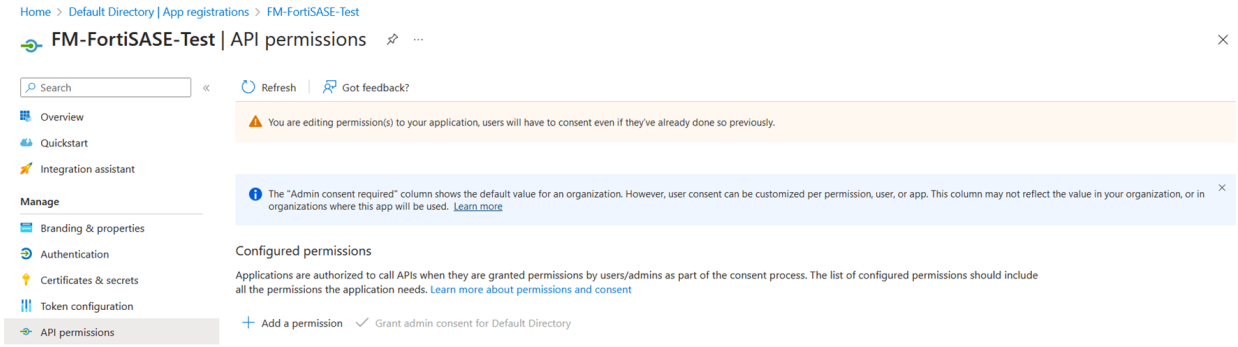
Before you can autoconnect to VPN using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

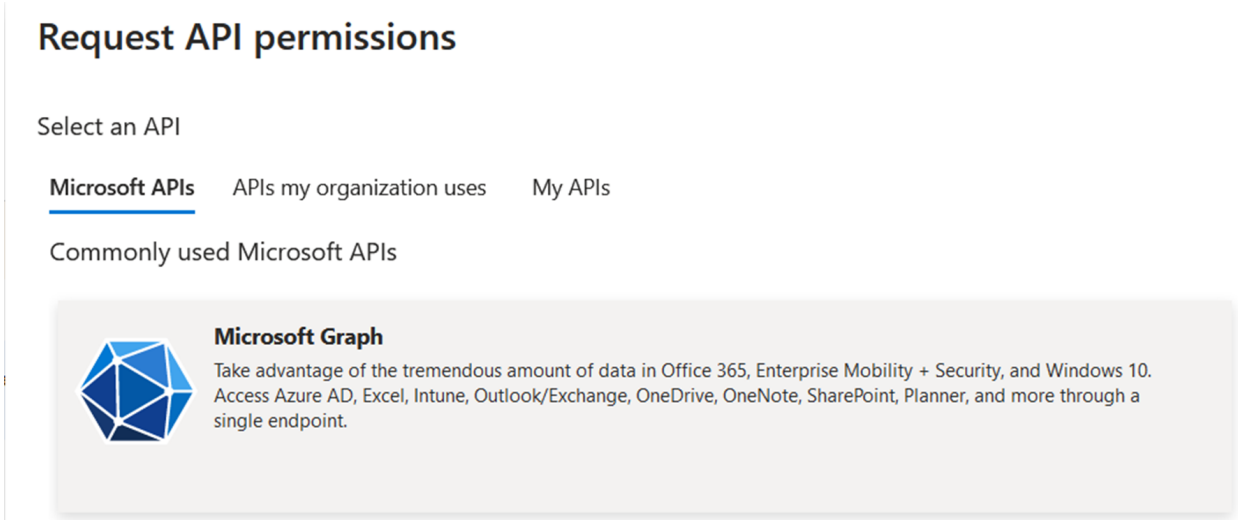
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

To add Microsoft Graph API application permissions required for autoconnect and searching user groups:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.

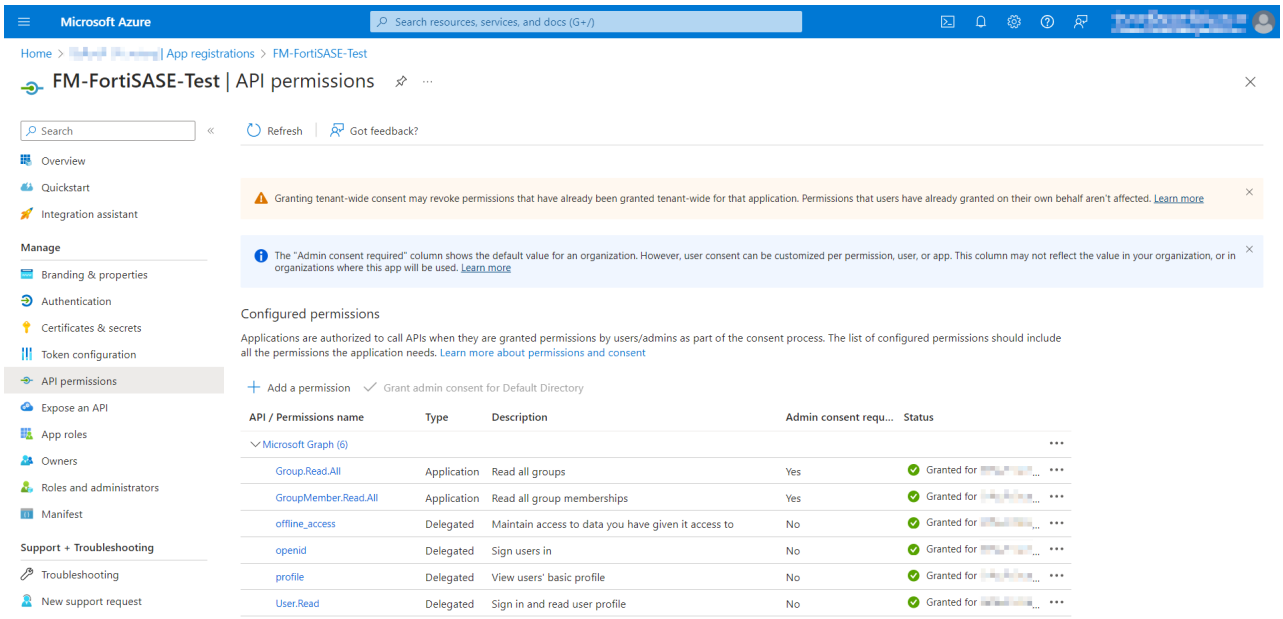


4. In the *Request API permissions* slide-in, click *Microsoft Graph*.



5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*\
   c. Click *Add permissions*.

6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
      - *Openid permissions > offline_access – Maintain access to data you have given it access*
      - *Openid permissions > openid – Sign users in*
      - *Openid permissions > profile – View users' basic profile*
      - *User > User.Read – Sign in and read user profile*
7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent* confirmation prompt. Observe the *Grant consent successful* notification at the top-right.
   Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.



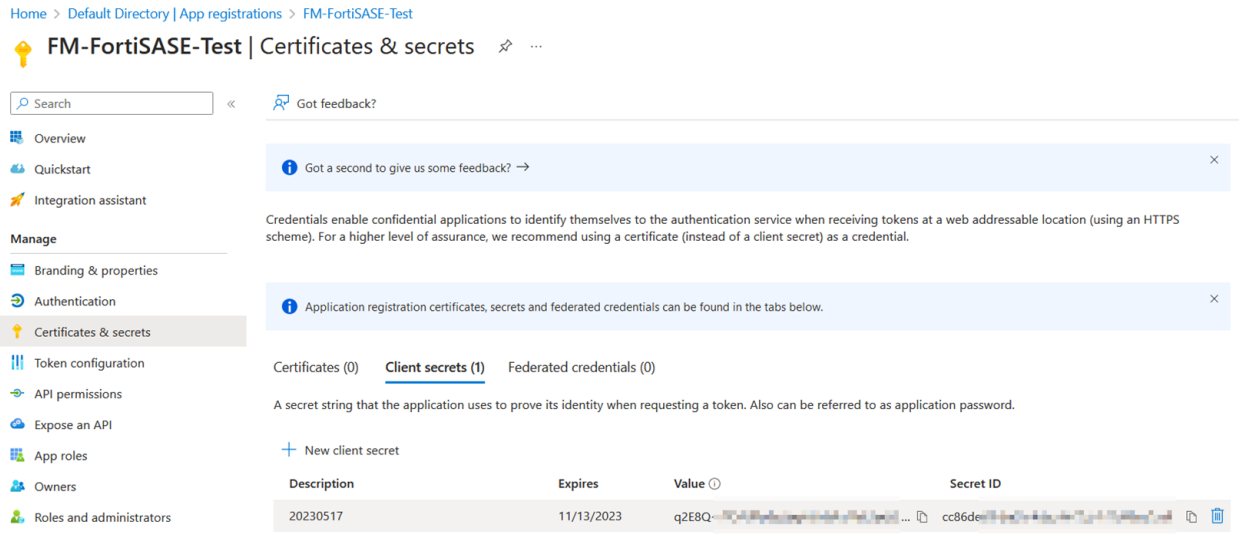
This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.

Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

Feature	API permission group	Permission name	Type
VPN autoconnect	*OpenId permissions*	*offline_access*	Delegated
	OpenId permissions	*openid*	
	OpenId permissions	*profile*	
	User	*User.read*	
Group searching	*Group*	*Group.Read.All*	Application
	GroupMember	*GroupMember.Read.All*	

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

Searching user groups from Entra ID SSO

After performing preliminary steps and determining the Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) single sign on (SSO) credentials, you can proceed to configure them in FortiSASE to allow dynamic group discovery from Entra ID SSO and select a group for SAML group matching.

The following example is for searching user groups from Entra ID SSO from FortiSASE for a FortiClient agent-based mode SSO configuration and demonstrates general steps that also apply to a secure web gateway mode SSO configuration.

To search user groups from Entra ID SSO in FortiClient agent-based mode:

1. Go to *Configuration* > *VPN User SSO*.
   a. For a new configuration, enter the Entra ID SSO fields.
   b. For an existing configuration, click the pencil icon to the right of *Identity Provider Configuration*.
2. Select *SAML Group Matching* and click *Search*.
3. From the *SAML Provider Type* dropdown list, select *Entra ID*. Next to *SAML Provider Credential*, click *Change*.
4. Enter the Entra ID credentials obtained from the Entra ID portal:
   - Tenant ID
   - Client ID
   - Client Secret
5. Click *OK* to save the credentials.
6. Click *Select group* next to *SAML Remote User Groups* and notice that the groups are dynamically obtained from Entra ID and populated. Select a remote user group from the table and click *OK* to save the changes.
7. Notice that the *Configure Service Provider* page has the *Group Name* automatically filled in with the selected user group's name. Click *Next* to advance this page and click *Submit* on the *Review* page to submit the VPN user SSO configuration settings.

Testing SSO configuration from FortiSASE

From FortiSASE, you can test the single sign on (SSO) configuration settings end-to-end by logging into a user account configured on your SSO server. This feature allows you to open a popup test window that points to the SSO login page.

This test provides SSO configuration test results and raw log output of SAML debug from the security PoP that can help you troubleshoot issues with any misconfigured SSO configuration settings.

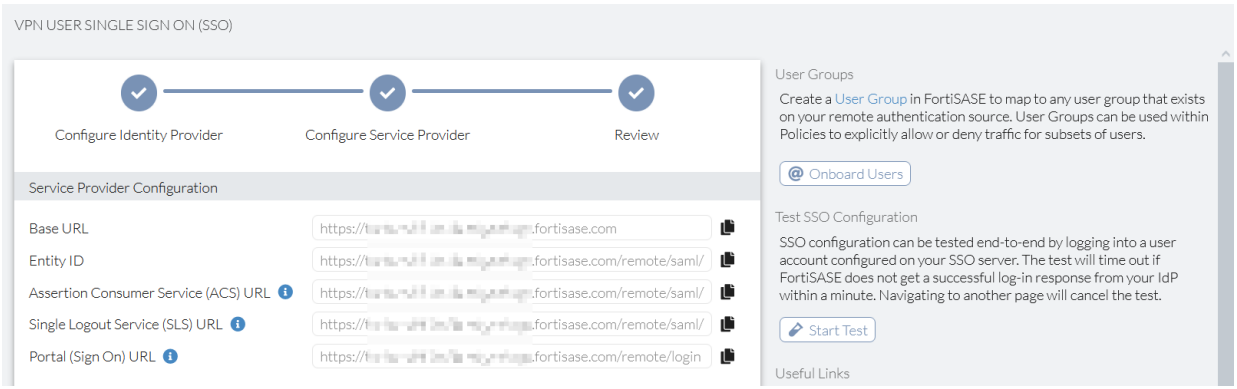
When using the Chrome web browser for testing SSO configuration, you must disable *TLS 1.3 hybridized Kyber support* via *chrome://flags* for this test to work.

Testing SSO configuration from FortiSASE supports FortiClient agent-based mode using Microsoft Entra ID SSO or Okta SSO via *Configuration* > *VPN User SSO*.

The example below is for testing an Entra ID SSO configuration and demonstrates general steps that also apply to Okta SSO.

To test SSO configuration from FortiSASE using Entra ID SSO:

1. Go to *Configuration* > *VPN User SSO*. Ensure that you configured Entra ID SSO and that you clicked *Submit* at the end of the configuration steps. For details, see Configuring FortiSASE with Entra ID SSO in FortiClient agent-based mode on page 211.
2. In right-hand gutter, click *Start Test*.



Ensure that you disable or exempt any web browser popup blockers to allow popups for the *Configuration* > *VPN User SSO* page prior to clicking *Start Test*. Otherwise, you see the error message *Failed to trigger SSO configuration test* and the test SSO configuration feature does not work as desired.

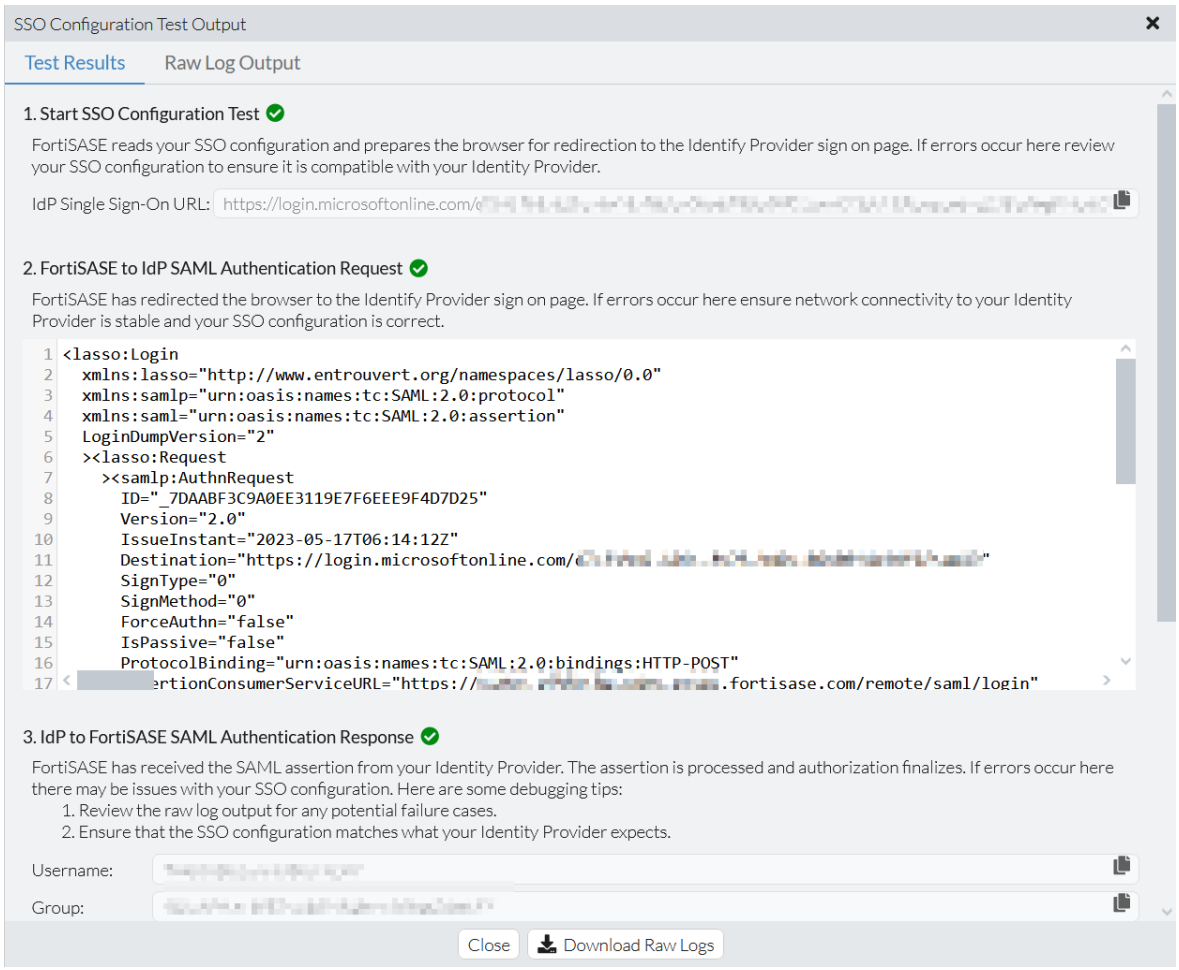
Ensure that the web browser remains on the *Configuration* > *VPN User SSO* page for the test duration. Going to another page cancels the test.

3. A popup from the SSO provider prompts for login information. This is the user account that has already been set up on the SSO server that you want to use for the test. When prompted, enter the username and password of the user account to use for the test.

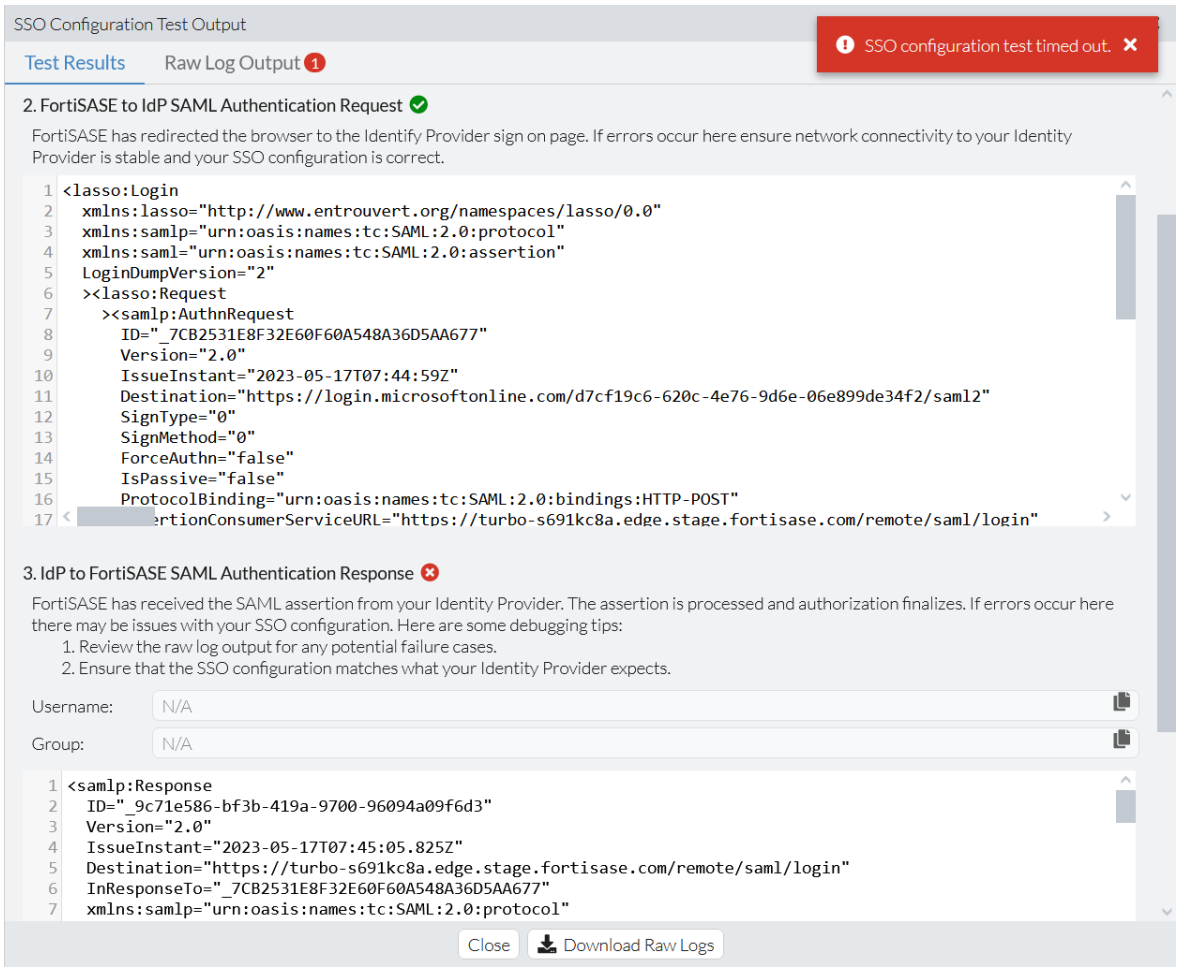
Ensure that you enter the username and password of the user account within one minute. The test times out if FortiSASE does not get a successful login response within a minute with the error message *SSO configuration test timed out*.

4. You see that the notification *SSO configuration verified successfully* displays in the right-hand gutter when the SAML connection test succeeds. If the test fails, one of the following error messages displays:
   - *Failed to trigger SSO configuration test.*
   - *SSO configuration test timed out.*
   - Within one minute of starting the test, the *SSO Configuration Test Output* slide-in window appears.
     i. In the *Test Results* tab, you see the corresponding icons that help you to narrow down your SAML troubleshooting steps:
        - Green checkmark next to test steps that succeeded
        - Red X next to test steps that failed, which suggests issues with the SSO configuration. The window displays debugging/troubleshooting steps when this occurs.

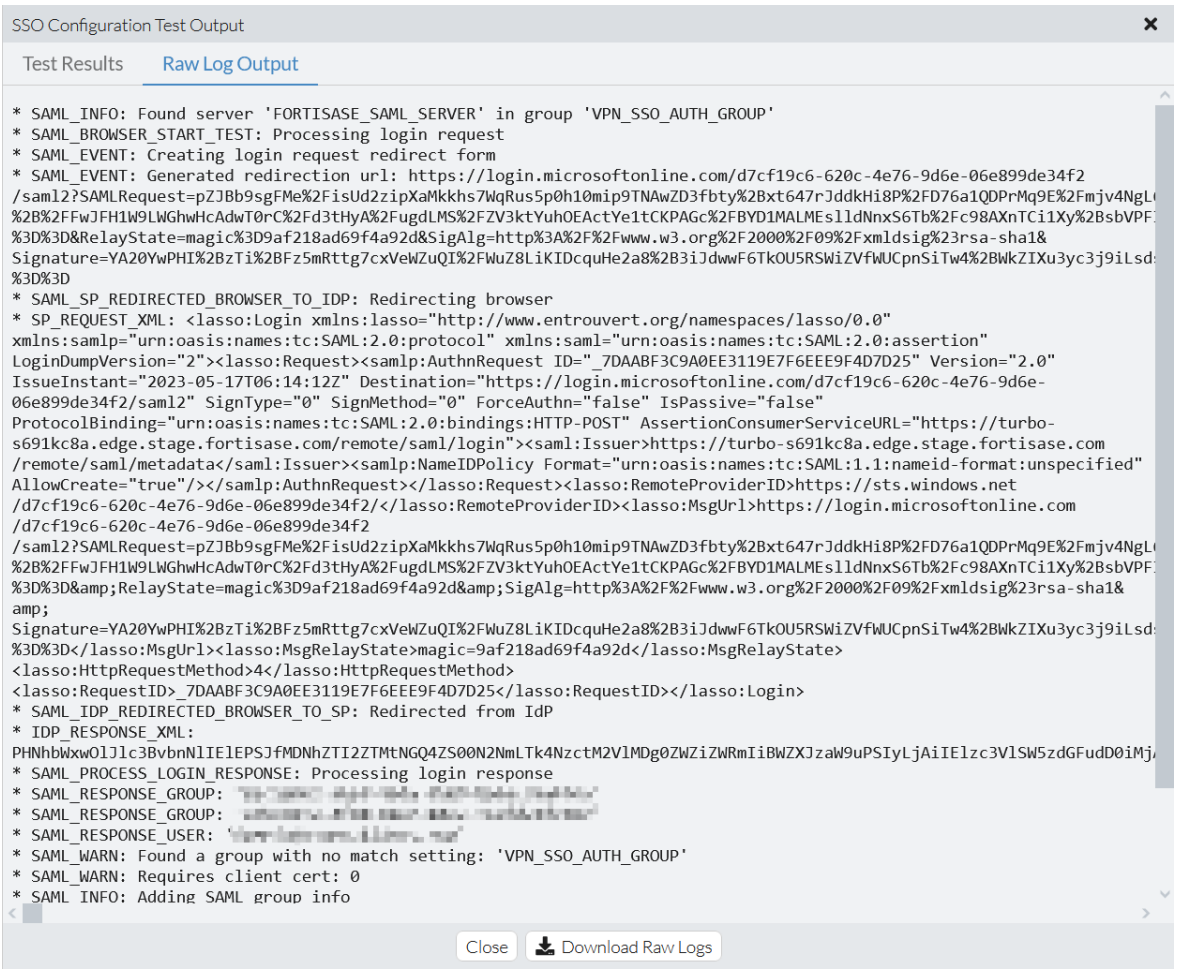
     The following shows an example *Test Results* tab with successful test steps.



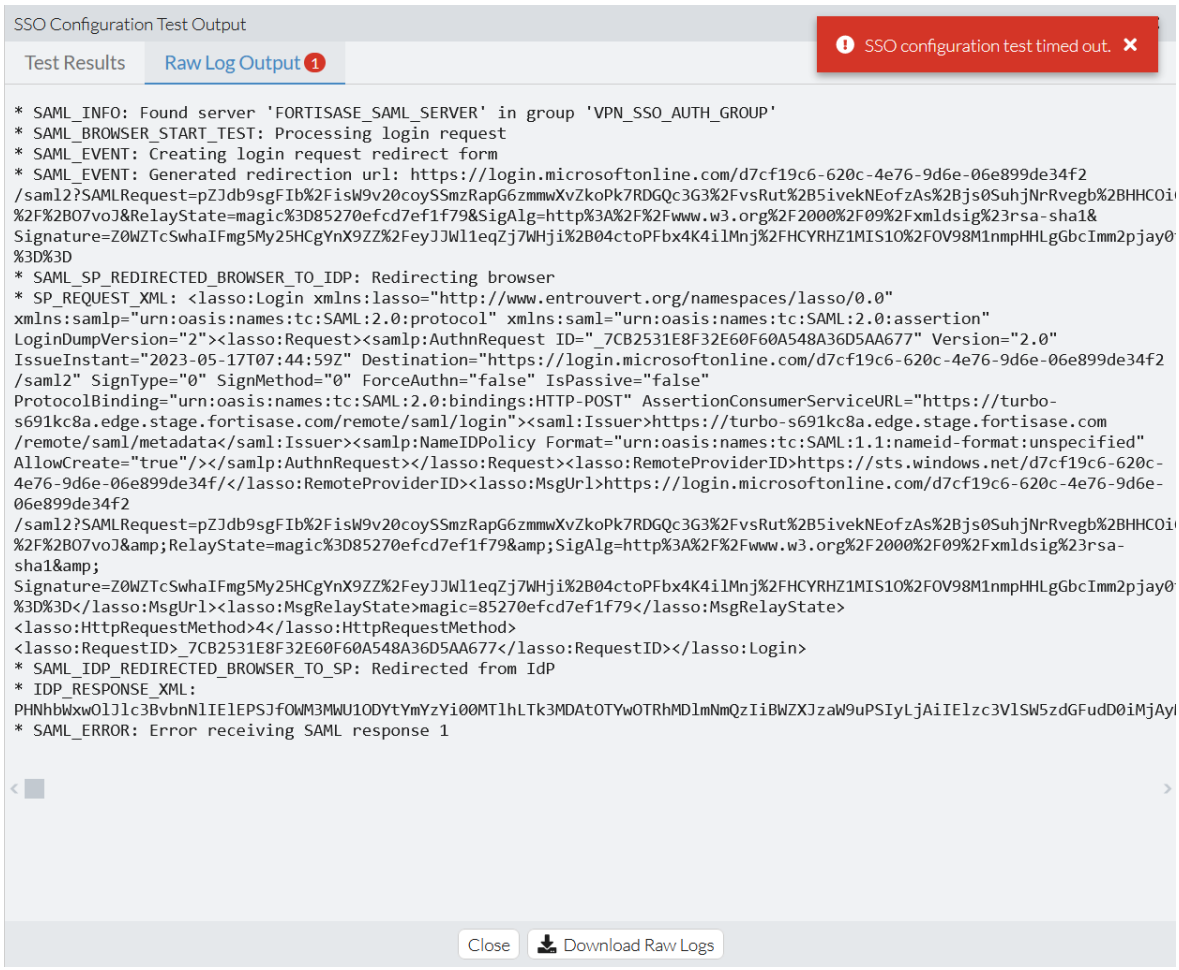
The following shows an example *Test Results* tab with a failed test step that an identity provider entity ID misconfiguration caused.



ii. In the *Raw Log Output* tab, observe the SAML debug raw log output from the security point of presence with sensitive information removed. The following shows an example of the *Raw Log Output* tab with successful test steps.



The following shows an example *Raw Log Output* tab with a failed test step that an identity provider entity ID misconfiguration caused.



Notice the number next to the *Raw Log Output* tab title indicating the number of error messages in the output. See the *SAML_ERROR: Error receiving SAML response 1* as the last line of the output.

Users

To create a local VPN user:

1. Go to *Configuration* > *Users & Groups*.
2. Click *Create*.
3. Select *User*, then click *Next*.
4. In the *Email* field, enter the desired email. FortiSASE sends instructions and an invitation code to this email address. The user uses this code to connect FortiClient to FortiSASE.
5. If desired, enable and configure *Temporary administrative password*. 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.
6. Click *OK*.

To create a user group:

1. Go to *Configuration* > *Users*.
2. Click *Create* > *User Group*.
3. In the *Members* field, click +.
4. In the *Select Entries* pane, select the desired users to add to this user group.
5. In the *Remote Groups* field, select *Create*.
6. From the *Remote Server* dropdown list, select the desired server.
7. In the *Groups* field, add the desired groups from the selected server to this user group. Click *OK*.
8. Click *OK*.

To import users in bulk using a CSV file:

1. Go to *Configuration* > *Users*.
2. Click *Import/Export* > *Import Users*.
3. In the *Import Users* pane, click *Browse*.
4. Browse to and upload the CSV file that contains the desired email addresses. Click *Next*.
5. The *Import Users* pane displays the email addresses that it detected in the CSV file after removing those already associated with existing VPN users. Review the email address list.
6. Click *Import*. The imported users display on the *VPN Users* page.

PKI

A public key infrastructure (PKI) user are users identified by a digital certificate.

PKI users are used to define peer users and are used with SPA Service Connections using IPsec VPN when *Authentication Method* is configured as *Certificate*.

To create a PKI user:

1. Go to *Configuration* > *PKI*.
2. Click *Create*.
3. In the *Name* field, enter the name of the PKI user.
4. (Optional) In the *Subject* field, enter the peer certificate name constraints. This is field can be empty, can contain only the CN value or can contain a substring of the certificate subject.

   For example, if the actual subject of the peer certificate is set to "C = CA, CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC, emailAddress = dc1@mycompany.com", you can configure then the *Subject* field with one of the following values:
   - Empty
   - "CN = dc1"
   - Substring of the whole subject:
     - "CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC, emailAddress = dc1@mycompany.com"

       OR
     - "C = CA, CN = dc1, L = VAN, O = MyCompany, OU = it, ST = BC"
5. For the *CA* dropdown list, specify which certificate FortiSASE uses to validate the peer's certificate. This can be any CA in the peer's certificate chain. You may need to upload a remote CA certificate to FortiSASE specifically to

identify PKI peer users. See Certificates on page 268.

6. Click *OK*.

See Configuring a new service connection on page 94 for details on how to configure a defined PKI user.

Endpoints

In *Endpoints*, you can define the configuration of FortiClient software on endpoints. You can also monitor endpoint statuses and deregister endpoints.

Endpoint features do not apply for secure web gateway mode users. See SWG agentless mode on page 15.

Profiles

FortiSASE supports multiple endpoint profiles to provide granular behavior for different user types that belong to an Active Directory (AD) group or a non-AD group, such as:

- IT can disconnect from always-on VPN.
- Marketing can use removable media and authenticates using LDAP.
- All other users cannot disconnect from always-on VPN or use removable media, and authenticate using single sign on (SSO).

Configuration > *Profiles* presents a table of profiles, with the *Default* profile assigned to all other users if you have not defined custom profiles. You cannot delete the *Default* profile.

You can prioritize and assign endpoint profiles to on-net endpoints based on matching AD domain users and groups or you can assign endpoint profiles based on endpoints assigned to different non-AD groups.

Viewing users and groups from an AD server requires an AD connection in *Configuration* > *Domains*. LDAP user and group information is shared with the FortiSASE Endpoint Management service, which assigns profiles to endpoints that are locally connected to the LDAP domain whenever domain users are logged in by matching selected users or groups.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

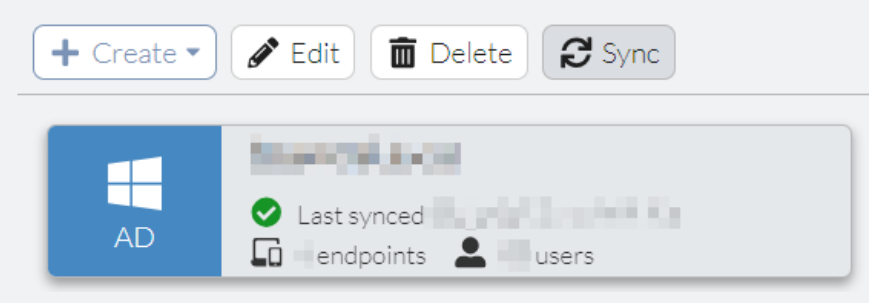
FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

In *Configuration >Domains*, click an AD domain card and click *Sync* to synchronize the AD connection with any updates from the AD server, if necessary:



When creating a new endpoint profile, you can use the *Groups & AD Users* tab to select which AD users/groups or non-AD groups you will apply the profile to, and you can use an option in the *Connection* tab to enable/disable SSO authentication per profile. To assign endpoints to different non-AD groups, see Groups & AD Users on page 253.

To configure Profiles options:

1. Go to *Configuration* > *Profiles*.
2. Click *Create* or edit an existing profile.
3. In the *Name* field, enter the desired name of the endpoint profile.
4. Configure the options on each tab as the following topics describe:
   - Connection on page 246
   - Protection on page 250
   - Sandbox on page 251
   - ZTNA on page 253
   - Groups & AD Users on page 253
   - Settings on page 255

Connection

To configure the Connection tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Connection* tab, to enable VPN autoconnect, for *Endpoint connects to FortiSASE VPN*, select *Automatically*. Disable the toggle for *Show button to disconnect from FortiSASE VPN* to prevent endpoints from being able to disconnect from FortiSASE's secure internet access (SIA) VPN.
   To let endpoint users manually connect to FortiSASE's SIA VPN, select *Manually* under *Endpoint connects to FortiSASE VPN*. This disables the autoconnect feature to connect to FortiSASE's SIA VPN.
3. Under *FortiSASE bandwidth optimization*, enable *Bypass FortiSASE when endpoint is on-net*.
   On-fabric rule sets determine if FortiSASE considers endpoints trusted or on-fabric, meaning they are in a corporate network which should have some level of on-premise security and do not need to automatically connect to FortiSASE VPN for security inspection. This also helps to optimize FortiSASE bandwidth usage.
   For example, when you add an on-fabric rule set using your corporate network's public IP address, the endpoints on this network do not automatically connect to FortiSASE VPN when they are on-fabric. Therefore, endpoints only autoconnect to FortiSASE VPN when they have public IP addresses that do not match the configured trusted public IP addresses, meaning when they are considered untrusted or off-fabric and require FortiSASE security inspection.
   FortiSASE supports on-fabric rule sets with the following detection types to determine if an endpoint is connecting from a trusted location:

Detection type	Description
Connects with a known public IP	In the *Known public (WAN) IP addresses* field, enter the desired IP address. You can configure multiple addresses using the + button. FortiSASE supports configuration of single IP addresses and IP subnets. FortiSASE considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified.
Is connected to a known DNS server	In the *Known server IP addresses* field, configure at least one IP address for the desired DNS server. You can configure multiple IP addresses using the + button. FortiSASE considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration.
Is connected to a known DHCP server	When *Identify servers by IP/MAC addresses* is enabled, configure the IP and/or MAC address for the desired DHCP server in the *Known server IP addresses* and *Known MAC addresses* fields, respectively. If configuring the *Identify servers by IP/MAC addresses* option, the *MAC Address* field is optional. When *Identify servers by DHCP option 224* is enabled, configure the DHCP code for the desired DHCP server. If the DHCP server is a FortiGate, then you can use the FortiGate serial number as the DHCP code, if desired. Otherwise, the DHCP code can be any string configured in the DHCP server as option 224.

Detection type	Description
	You can configure just the Identify servers by IP/MAC addresses option, just the Identify servers by DHCP option 224 option, or both options. You can configure multiple IP and MAC addresses and DHCP codes using the + button on each tab. FortiSASE considers the endpoint as satisfying the rule if it is connected to a DHCP server that matches the specified configuration.
Connects from a known local subnet	In the *Known subnets* field, enter a range of IP addresses. In the *Known gateway MAC addresses* field, optionally enter the default gateway MAC address. Configuring the MAC address is optional. You can configure multiple addresses using the + button. FortiSASE considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified and if its default gateway MAC address matches the one specified, if it is configured.
Can ping a known server	In the *Known server IP addresses* field, enter the server IP address. You can configure multiple addresses using the + button. FortiSASE considers the endpoint as satisfying the rule if it can access the server at the specified IP address.

Starting in 24.2.c, FortiSASE supports configuring a known IP subnet for the public IP detection type used with on-fabric rule sets. This feature requires FortiClient 7.0.13 and above. Administrators can no longer configure IP ranges for the public IP on-fabric detection type. A previously configured public IP range will be displayed as the underlying multiple single public IP addresses within the IP range.

Configure an on-fabric rule set to prevent auto connect to FortiSASE VPN when endpoints are on-net:

a. Next to *Bypass FortiSASE when endpoint is on-net*, click the dropdown and click + to create a new on-fabric rule set.
b. In the *Create new rule set* slide-in, select one or more detection types by toggling them.
c. Configure the required fields as described for each detection type.
d. Click *OK* to save the on-fabric rule set.
e. Click *OK* to select the newly created on-fabric rule set.
f. Click *OK* to save the profile configuration.

On-fabric rule sets can also be created, edited, and deleted in *Configuration* > *Profiles* from the *On-fabric rule sets* tab. From this tab, you can also view which profiles each rule set is used in.

4. Under *FortiSASE bandwidth optimization*, configure *Split tunneling destinations*. Traffic configured as a split tunneling destination considered to be a trusted destination that is excluded from the FortiSASE VPN tunnel and redirected to the endpoint physical interface by passing FortiSASE. This also helps optimize FortiSASE bandwidth usage. For example, you may want to add a high bandwidth-consuming application, such as Microsoft Teams or Zoom, as a split tunneling destination. Configure a split tunneling destination:

a. Click *Create*.

b. Configure the following fields:

Option	Description
Type	Select *Infrastructure*, *FQDN*, *Local Application*, or *Subnet*.

Match	• If you selected *Infrastructure*, select the desired application from the dropdown list.
	• If you selected *FQDN*, enter or select the desired fully qualified domain name (FQDN). The FQDN resolved IP address is dynamically added to the route table when in use, and is removed after disconnection. For example, if you want to exclude YouTube from the VPN tunnel, you can enter youtube.com. When endpoint users use any popular browser such as Chrome, Edge, or Firefox to access youtube.com or *.youtube.com, this traffic does not go through the VPN tunnel.
	• If you selected *Local Application*, specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon.
	For example, to exclude Microsoft Teams and Firefox from the VPN tunnel, you can enter any of the following combinations:
	  • **Application Name**: teams.exe;firefox.exe
	  • **Full Path**: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe
	  • **Directory**: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\
	To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column.
	• If you selected *Subnet*, enter the desired subnet. The subnet is dynamically added to the route table when in use, and is removed after disconnection.
	You can select host groups when using the *Subnet* match type. You must create host groups in *Configuration* > *Hosts* before they become visible in the *Create Destination* dialog.

You cannot create subnet destinations in a custom endpoint profile. Therefore, subnet destinations defined in the *Default* profile also apply to all custom profiles.

FortiSASE does not support wildcard FQDNs when configuring an FQDN split tunneling destination.

c. Click *OK*.

5. Under *VPNs available to users*, you can configure a custom IPsec or SSL VPN configuration or edit the default SSL VPN configuration for *Secure Internet Access*. These configurations are typically useful for use cases that require

endpoints to connect to an on-premise FortiGate via VPN.

In FortiSASE 24.1.c and older versions, *Authenticate with SSO* was previously located in the *Settings* tab.

In FortiSASE 24.2.a and later, you can find *Authenticate with SSO* in the *Connection* tab, in *VPNs available to users*, and by collapsing *Advanced Settings*. Also, in FortiSASE 24.2.a and later, you can edit the default SSL VPN *Secure Internet Access* configuration.

To create an alternative custom VPN, do the following:

a. Click *Create*, and select *SSL VPN* or *IPsec VPN* as per your requirement.

b. Enter the *Name* of the VPN tunnel.

c. Do one of the following:

- For an IPsec VPN tunnel, configure the following settings:

Field	Value
Remote gateway	Remote gateway FQDN or IP address.
Authentication method	Select preshared key, smart card certificate, or system store certificate to connect to the IPsec VPN gateway.
Prompt for username	Display a prompt for the end user to enter their username and password for user authentication.
Advanced settings	Enable the toggle for required options to be visible on FortiClient. When you enable *Authenticate with SSO*, FortiClient is enabled with SSO as an authentication option and uses its built-in browser agent.

- For an SSL VPN tunnel, configure the following settings:

Field	Value
Remote gateway	Remote gateway FQDN or IP address.
Port	SSL VPN port number.
Require certificate	Enable to use certificate-based user authentication.
Prompt for username	Display a prompt for the end user to enter their username and password for user authentication.
Advanced settings	Enable the toggle for required options to be visible on FortiClient. When you enable *Authenticate with SSO*, FortiClient is enabled with SSO as an authentication option and uses its built-in browser agent. To use an external browser, enable *Use external browser as user-agent for SAML login*.

FortiSASE supports authentication using multiple SSO providers using FortiTrust Identity. See Configuring FortiSASE with FortiTrust ID as SAML IdP proxy for Entra ID SSO on page 227.

6. The SSL VPN settings apply to alternative SSL VPN tunnels. Enable the respective options to prevent connection errors on FortiClient due to invalid SSL certificates installed on the on-premise VPN gateway.

To enable VPN autoconnect on FortiClient for alternative or custom VPN tunnels, set *Endpoint connects to FortiSASE VPN* to *Manually* and under required alternative or custom VPNs, enable *Show Auto Connect* under *Advanced Settings* for individual alternative VPN tunnel configurations. If the VPN connections fails, the VPN does not automatically connect to the backup FortiSASE SIA VPN. Endpoint users must then manually connect to FortiSASE SIA VPN.

When *Endpoint connects to FortiSASE VPN* is set to *Manually*, you can configure FortiSASE to provide an option to the end user to save their VPN login password with or without SAML configured under *VPNs available to users* > <*VPN tunnel*> > *Advanced settings*. When using SAML authentication, feature of saving password relies on persistent sessions being enabled in the identity provider (IdP), discussed as follows:

- Azure
- Okta

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt.

7. You must configure some more important FortiClient settings on the *Settings* tab. See Settings on page 255.

Protection

To configure the Protection tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Protection* tab, in *Malware*, configure the following:
   a. Enable *Next Generation AntiVirus*. This feature includes real-time protection against viruses, as well as cloud-based malware detection. Cloud-based malware protection protects endpoints from high risk file types from external sources such as the internet or network drives by querying FortiGuard to determine whether files are malicious. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.
   b. Enable *Anti-Ransomware*. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient. Antiransomware protects all content in the selected folders against unauthorized changes. You can click *Create* to add a custom directory. To remove a folder, select it then click the *Delete* button.
3. FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities. You can view a summary of endpoint vulnerability information on the Dashboard.
   On the *Protection* tab, in *Scan for Vulnerabilities*:
   a. Enable *Scheduled scanning* and select these settings:
      i. For *Schedule type*, select *Weekly* (default), *Daily*, or *Monthly*.
      ii. For *Scan on*, select *Sunday* (default), or specify a day from *Monday* through *Saturday* or *1st* through *31st*.
      iii. For *Start at*, specify the desired time to start the scan.

b. Enable *Event-based scanning*. This feature automatically scans for vulnerabilities when the following occur:
   - Endpoint connects to FortiSASE.
   - Endpoint OS is updated.
   - Vulnerability signatures are updated.

4. On the *Protection* tab, in *Removable Media Access Control*, configure the following:
   a. For *Default Removable Media Access Control*, select *Allow* (default), *Block*, or *Monitor*. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.
   b. Enable *Notify Endpoint of Blocks* to display a bubble notification when FortiClient takes action with a removable media device.
   c. In *Access Control Rules*, click *Create* to create a removal media access rule. Configure the following fields. For the class, manufacturer, vendor ID, product ID, and revision, you can find the desired values for the device in one of the following ways:
      - Microsoft Windows Device Manager: select the device and view its properties.
      - USBDeview

Option	Description
Type	Select *Simple* or *Regex* for the rule type. When *Simple* is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions. When *Regex* is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.
Action	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: • *Allow*: Allow access to removable media devices connected to the endpoint that match this rule. • *Block*: Block access to removable media devices connected to the endpoint that match this rule.
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.

   d. Click *OK*.

Sandbox

To configure the Sandbox tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.

2. On the *Sandbox* tab, configure the following. This feature only works for endpoints where Sandbox Detection was enabled when installing FortiClient. Configure the following options:

Options	Description
Sandbox Mode	Select *FortiSASE* to configure connection to FortiSASE Sandbox or *Standalone FortiSandbox* to configure connection to an on-premise standalone FortiSandbox.
IP address/Hostname	For a standalone FortiSandbox, enter the FortiSandbox's IP address, FQDN, or hostname.
Username	Optional. Enter the FortiSandbox username. This option is only available for a standalone FortiSandbox.
Password	Optional. Enter the FortiSandbox password. This option is only available for a standalone FortiSandbox.
Region	FortiSASE Sandbox region.
Time Offset	FortiSASE Sandbox time offset.
File Submission Options	
All Files Executed from Removable Media	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
All Files Executed from Mapped Network Drives	Submit all files executed from mapped network drives.
All Web Downloads	Submit all web downloads.
All Email Downloads	Submit all email downloads.
Remediation Actions	
Action	Choose *Quarantine* or *Alert & Notify* for infected files. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the *Sandbox Detection Verdict Level* setting.
Sandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the *Action* field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if *Action* is configured as *Quarantine* and *FortiSandbox Detection Verdict Level* is configured as *Medium*, FortiClient quarantines all infected files that FortiSandbox detects as Medium or a higher level (High or Malicious). FortiClient does not quarantine files for which FortiSandbox returns a verdict below this level (Low Risk or Clean).
Exceptions	
Exclude Files from Trusted Sources	Exclude files signed by trusted sources from FortiSandbox submission. Following is a list of sources that FortiSandbox trusts: • Microsoft • Fortinet • Mozilla • Windows

Options	Description
	• Google • Skype • Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion list.

ZTNA

FortiSASE supports a maximum of 32000 ZTNA connection rules.

To configure the ZTNA tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *ZTNA* tab, configure Zero Trust Network Access (ZTNA) rules as desired:
   a. Click *Create*.
   b. In the *Rule Name* field, enter the desired name.
   c. In the *Destination Host* field, enter the IP address/FQDN and port of the destination host in the format <IP address or FQDN>:<port>. For example, you could enter demo.fortinet.com:22 as the destination host value.
   d. In the *ZTNA Access Proxy* field, enter the access IP address and port of the FortiGate acting as the access proxy in the same format. For example, you could enter 21.14.22.11:80 as the proxy gateway value.
   e. Enable or disable *Encryption*. By default, *Encryption* is disabled. When *Encryption* is enabled, traffic between FortiSASE and the FortiGate is always encrypted, even if the original traffic has already been encrypted.
   f. If desired, enable *Use External Browser for SAML Authentication*. FortiSASE can use a browser as an external user agent to perform SAML authentication instead of using the FortiClient console.
   g. Click *OK*.

Groups & AD Users

To configure the Groups & AD Users tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Groups & AD Users* tab, you can select Active Directory (AD) users, non-AD groups, or AD groups to assign the endpoint profile to.

Viewing users and groups from an AD server requires configuring an AD connection in *Configuration* > *Domains*. See Domains on page 263.

The FortiSASE Endpoint Management Service does not support importing LDAP subdomains if you have already imported the LDAP parent domain previously into it.

FortiSASE can connect to DNS, RADIUS, or LDAP servers with internal IP addresses or FQDNs if you set *Access Type* to *Private* in the RADIUS or LDAP server settings, internal servers are located behind a secure private access (SPA) hub, and the SPA hub in FortiSASE has been configured with BGP per overlay.

Implicit and split DNS rules for VPN traffic configured with internal IP addresses work with SPA hubs configured with any BGP routing design.

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

See Network restrictions removed on page 23.

3. Click *Add* and select *AD Users* or *Groups* as per your requirements:
   - When selecting *AD Users*, a slide-in appears, which allows you to view the domains corresponding to configured AD servers. You can collapse the LDAP domain and select AD users from the list of AD users.
   - When selecting *Groups*, do one of the following:

Group type	Description
AD groups	A slide-in appears that allows you to view the domains corresponding to configured AD servers and select AD groups. To select AD user groups, you can collapse the LDAP domain using the + button and select the required AD groups from a tree view of groups using the toggle.
Non-AD groups	A slide-in appears that allows you to create nested non-AD user groups under *Non-AD Groups* and assign endpoints to the group. To configure a non-AD user group and add endpoints to the newly created non-AD group, do the following: **1.** Collapse *Non-AD Groups* using the + button. **2.** Select the group under that you want to create a group under and click *Create sub-group*. **3.** Enter the *Name* of the group as desired. **4.** Select the available non-AD endpoints to add to the group. Click *Add selected*. **5.** Click *OK*. **6.** Only enable the toggle of the specific group to assign the profile to. **7.** Click *OK*.

4. Click *OK*.

5. Repeat step 3 to add more groups and AD users. If you add more groups to the list, the endpoint user must be a part of at least one group for FortiSASE to assign the profile to the endpoint.
6. Click *OK* to save the endpoint profile.
7. To view the endpoints that are assigned to a profile, click the profile and select *View Endpoints* from the tool bar.

Settings

To configure the Settings tab:

1. Create a new profile or edit an existing one:
   a. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected.
   b. Click *Create* or edit an existing profile.
   c. In the *Name* field, enter the desired name of the endpoint profile.
2. On the *Settings* tab, configure the following:

In FortiSASE 24.1.c and older versions, *Authenticate with SSO* was previously located in the *Settings* tab.

In FortiSASE 24.2.a and later, you can find *Authenticate with SSO* in the *Connection* tab, in *VPNs available to users*, and by collapsing *Advanced Settings*.

   a. Enable or disable *Show tags on FortiClient*. When enabled, the end user can view the tags applied on their endpoint.
   b. Enable or disable *Show notifications for device status, telemetry, and management*. When enabled, the endpoint displays notifications for device status, telemetry, and management events such as when policies are installed, action is taken with a removable media device, etc.
   c. Enable or disable *Notify endpoint of VPN connectivity issues*. When enabled, a notification displays to the end user when FortiClient cannot connect to FortiSASE VPN.
   d. Under *Debugging options*, when you enable *Endpoints can disconnect from FortiSASE*, FortiClient's *Zero Trust Telemetry* tab shows a *Disconnect* option.
   Alternatively you can enable *Require disconnect password* and enter a password. When this option is configured, the endpoint user must enter the password on FortiClient to disconnect from the FortiSASE Management Service. You can use this option as an offline method of deregistering a FortiClient endpoint from the FortiSASE Management Service.

Example: Configuring a custom endpoint profile applied to an AD group

This example demonstrates how to configure a custom endpoint profile applied to an Active Directory (AD) group. It demonstrates how to configure an AD server that allows group matching, configure a custom endpoint profile to use this AD server to select a specific AD group with which this profile will be applied, and test that the correct profile is applied to an AD user within the selected AD group.

This example makes the following assumptions:

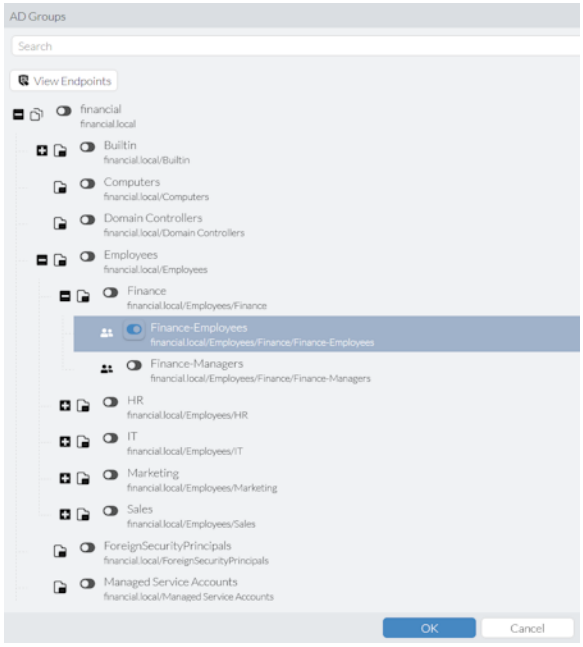
- The AD server has already been configured with AD services, AD users, and AD groups. The AD user johnlocus is a member of the Finance-Employees AD group.
- You have already configured SSO authentication on the SSO provider side and in FortiSASE.
- The endpoint used for testing the AD group matching is on-net, that is, locally on the same network as the AD server and joined to the AD domain.

- Default endpoint profile has been configured with *Authenticate with SSO* disabled to ensure that the configuration uses LDAP for VPN user authentication.
- You have already configured an AD connection. See To configure an AD connection: on page 263:

When the FortiSASE Endpoint Management Service uses AD servers with *Groups & AD Users* for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the *Server address* in the AD connection and may require some configuration or topology changes.

To configure a custom endpoint profile applied to an AD group:

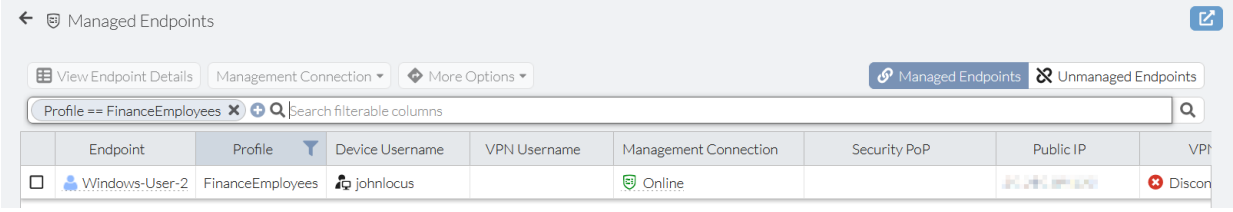
1. Go to *Configuration* > *Profiles* and click *Create*. By default, the *Profiles* tab is selected.
2. Add a name to the profile. For this example, use FinanceEmployees.
3. Go to the *Settings* tab and configure these settings:
   a. Enable *Show tags on FortiClient*.
   b. Enable *Notify endpoint of VPN connectivity issues*.
4. Go to the *Connection* tab and configure these settings:
   a. For *Endpoint connects to FortiSASE VPN*, select *Manually*.
   b. Enable *Show button to disconnect from FortiSASE VPN*.
   c. For *Alternative VPNs available to users*, select *Secure Internet Access* and click *Edit*. In *Advanced settings*, enable *Authenticate with SSO*.
5. Go to the *Groups & AD Users* tab to configure the AD group that the custom endpoint profile will apply to:
   a. Click *Add* > *AD Groups*. The LDAP domain and non-AD groups will be visible in the slide in window.
   b. To select the AD group, collapse the LDAP domain and select the desired AD group.



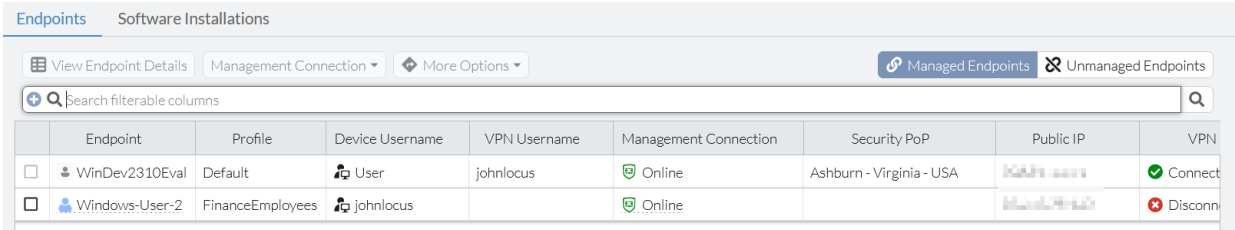
   c. Click *OK*.
   d. Review the selected AD group.
   e. Click *OK*.
   f. Observe that the newly created endpoint profile has an associated AD group and is enabled.

To test the custom endpoint profile is correctly assigned:

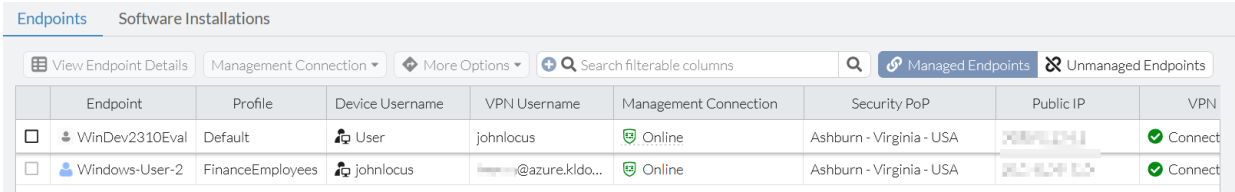
1. Log into the domain-joined endpoint using an AD user.
2. Go to *Configuration* > *Profiles*. By default, the *Profiles* tab is selected. Select the custom endpoint profile just created, and click *View Endpoints*. The *Managed Endpoints* view filtered with endpoints using the selected profile displays.



3. Alternatively, you can view all endpoints with different profiles using *Network* > *Managed Endpoints* under the *Endpoints* tab.



4. Establish a VPN connection on the test endpoint using SSO authentication.
5. Go to *Network* > *Managed Endpoints* under the *Endpoints* tab and observe the test endpoint VPN username indicates SSO authentication while another endpoint shows a VPN username indicating LDAP authentication. This demonstrates that SSO authentication and LDAP authentication can be used for VPN authentication of endpoints with different profiles.



Tagging

You can create zero trust network access tagging rules for Windows, macOS, Linux, iOS, and Android endpoints based on their OS versions, logged in domains, running processes, and other criteria. FortiSASE uses the rules to dynamically tag endpoints.

The following occurs when using tagging rules with FortiSASE and FortiClient:

1. FortiSASE sends tagging rules to endpoints.
2. FortiClient checks endpoints using the provided rules and sends the results to FortiSASE.
3. FortiSASE receives the results from FortiClient.
4. FortiSASE dynamically tags endpoints using the tag configured for each rule. You can view the dynamically tagged endpoints in *Configuration* > *Tagging*.

See Tagging rule types on page 259 for descriptions of all tagging rule types.

You can use tags to build dynamic policies that do not need to be manually reconfigured whenever endpoints statuses change. For example, consider that you want to block endpoints that are running Windows 7 and do not have antivirus (AV) running from accessing the internet. You would configure the following:

- A rule that applies a "Win7NoAV" tag to endpoints that are running Windows 7 and do not have AV running
- A policy that blocks endpoints with the Win7NoAV tag applied from accessing the internet.

As FortiSASE receives information from endpoints, it dynamically removes and applies the Win7NoAV tag to endpoints. For example, if an endpoint that previously had the Win7NoAV tag applied upgraded to Windows 10 and enabled the FortiClient AV feature, FortiSASE would automatically remove the Win7NoAV tag from the endpoint. That endpoint would then be able to access the internet.

The following instructions detail how to configure a dynamic policy that uses tags, using the Win7NoAV example:

To configure a dynamic policy using tags:

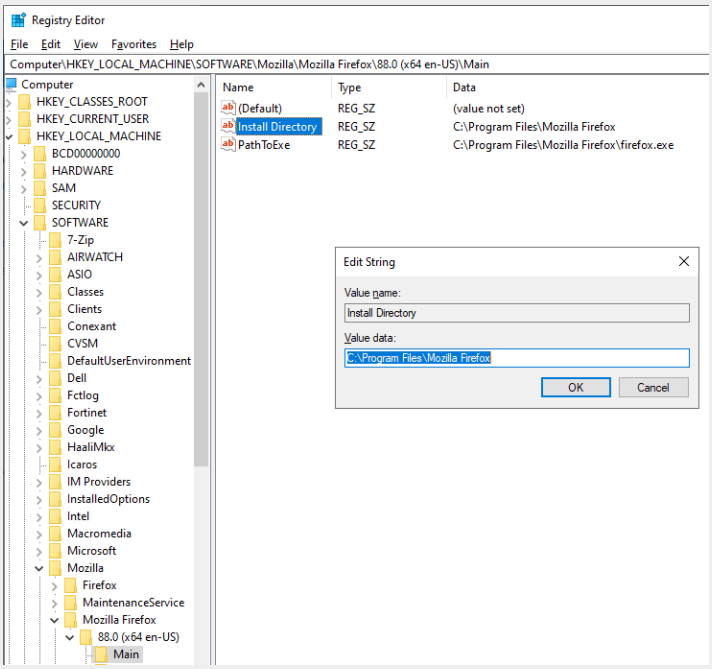
1. Configure the tagging rule set:
   a. Go to *Configuration* > *ZTNA Tagging*. Click the *ZTNA Tagging Rules* tab, then click *Create*.
   b. In the *Name* field, enter the desired rule set name.
   c. Toggle *Enabled* on or off to enable or disable the rule.
   d. (Optional) In the *Comments* field, enter any desired comments.
   e. Under *When the following rules match*, click *Create*.
   f. Configure the AV rule:
      i. For *OS*, select *Windows*.
      ii. From the *Rule Type* dropdown list, select *AntiVirus*.
      iii. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
      iv. Toggle *Negate* to *On*.
      v. Click *OK*.
   g. Configure the OS rule:
      i. For *OS*, select *Windows*.
      ii. From the *Rule Type* dropdown list, select *Operating System Version*.
      iii. From the *Operating System Version* dropdown list, select *Windows 7*.
      iv. Click *OK*.
   h. In the *Tag Name* dropdown list, create a tag named "Win7NoAV".
   i. Click *OK*.
2. Configure the tag as a source in a policy:
   a. Go to *Configuration* > *Policies*.
   b. Select the *Internet Access* or *Secure Private Access* tab to create an internet or private access policy, respectively.
   c. Click *Create*.
   d. In the *Source* field, click +. From the *Select Entries* panel, under *EMS Tag*, select the Win7NoAV tag.
   e. For *Destination*, select *All Internet Traffic*.
   f. For *Action*, select *Deny*.
   g. Click *OK*.

Tagging rule types

The following table describes tagging rule types and the OSes that they are available for. For all rule types, you can configure multiple conditions using the + button.

Rule type	OS	Description
User in AD Group	• Windows • macOS	From the *User in AD Group* dropdown list, select the desired Active Directory (AD) group that users should be members of. You can also use the *Negate* option for the rule to require that the user not be a part of the selected AD group. Viewing users and groups from an AD server requires an LDAP server configuration. The endpoint must satisfy all configured conditions to satisfy this rule.
AntiVirus	• Windows • macOS • Linux	From the *AntiVirus* dropdown list, select the desired conditions. You can require that an endpoint have antivirus (AV) software installed and running and that the AV signature is up-to-date. You can also use the *Negate* option for the rule to require that the endpoint does not have AV software installed or running or that the AV signature is not up-to-date. This rule applies for FortiClient AV. For Windows endpoints, this rule type also applies for third-party AV software that registers to the Windows Security Center. The third-party software notifies the Windows Security Center of the status of its signatures. FortiClient queries the Windows Security Center to determine what third-party AV software is installed and if the software reports signatures as up-to-date. The endpoint must satisfy all configured conditions to satisfy this rule.
Certificate	• Windows • macOS • Linux	In the *Subject CN* and *Issuer CN* fields, enter the certificate subject and issuer. You can also use the *Negate* option to indicate that the rule requires that a certain certificate is not present for the endpoint. FortiClient checks certificates in the current user personal store and local computer personal store. It does not check in trusted root or other stores. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require certificate A, certificate B, and not certificate C, then the endpoint must have both certificates A and B and not certificate C.
Domain	• Windows • macOS	In the *Domain* field, enter the domain name. If the rule is configured for multiple domains, FortiSASE considers the endpoint as satisfying the rule if it belongs to one of the configured domains.
EMS Management	• Windows • macOS • Linux • iOS • Android	FortiSASE considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry is connected.

Rule type	OS	Description
File	• Windows • macOS • Linux	In the *File* field, enter the file path. You can also use the *Negate* option to indicate that the rule requires that a certain file is not present on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C.
IP Range	• Windows • macOS • Linux • iOS • Android	In the *IP Range* field, enter the IP address, IP address range, or IP address with subnet. If multiple IP ranges and/or addresses are configured, FortiSASE considers the endpoint as satisfying the rule if its IP address matches one of the configured ranges or addresses.
Operating System Version	• Windows • macOS • Linux • iOS • Android	From the *Operating System Version* field, select the OS version. If the rule is configured for multiple OS versions, FortiSASE considers the endpoint as satisfying the rule if it has one of the configured OS versions installed. The following option is available for Windows: • *Enable latest update check*: FortiSASE checks if Windows OS updates were recently installed.
Registry Key	• Windows	In the *Key* field, enter the registry path or value name. End the path with \ to indicate a registry path, or without \ to indicate a registry value name. You can also use the *Negate* option to indicate that the rule requires that a certain registry path or value name is not present on the endpoint. This rule does not support using the value data. For example, the following shows a system where Firefox is installed. In this example, the registry path is `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main`. The value name is `Install Directory`, and the value data is `C:\Program Files\Mozilla Firefox`. You can configure a registry key rule to match `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main` as the path or `Install Directory` as the registry value name, but you cannot configure a rule to match `C:\Program Files\Mozilla Firefox`. Do not use square brackets when configuring this rule type.

Rule type	OS	Description
		 The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require registry key A, registry key B, and NOT registry key C, then the endpoint must have both registry keys A and B and not registry key C.
Running Process	• Windows • macOS • Linux	In the *Process Name* field, enter the process name. You can also use the *Negate* option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require process A, process B, and NOT process C, then the endpoint must have both processes A and B running and process C not running.
Sandbox	• Windows • macOS • Linux	From the *Sandbox Detection* dropdown list, select the desired condition. You can require that Sandbox detected malware on the endpoint in the last seven days. You can also use the *Negate* option for the rule to require that Sandbox did not detect malware on the endpoint in the last seven days.
Severity Level	• Windows • macOS • Linux	From the *Severity Level* dropdown list, select the desired vulnerability severity level.
User Identity	• Windows • macOS • Linux • iOS • Android	Under *User Identity*, select the following: • *User Specified*: endpoint user manually entered their personal information in FortiClient. • *Social Network Login*: endpoint user provided their personal information by logging in to their Google, LinkedIn, or Salesforce

Rule type	OS	Description
		account in FortiClient. You can further select one of the following: • *All Accounts*: all endpoints where the user logged in to the specified social network account type. • *Specified*: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts. FortiSASE considers the endpoint as satisfying the rule if it satisfies one of the conditions. You can also use the *Negate* option for the rule to require that the endpoint user has not manually entered user details or logged in to a social network account to allow FortiClient to obtain user details. FortiClient iOS does not support social network login with LinkedIn or Salesforce. FortiClient Android does not support social network login with Salesforce.
Windows Security	• Windows	From the *Windows Security* dropdown list, select the desired conditions. You can require that an endpoint have Windows Defender, Bitlocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows Firewall enabled. You can also use the *Negate* option for the rule to require that the endpoint have Windows Defender, Bitlocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows firewall disabled. The endpoint must satisfy all configured conditions to satisfy this rule.

For some rule types, such as the Running Process rule type, the endpoint must satisfy all conditions to satisfy the rule. There may be situations where you want FortiSASE to apply the same tag to endpoints that satisfy different conditions. Consider that you want FortiSASE to tag endpoints that are running Process A or Process B as "RP". In this case, you can create two rule sets: one for endpoints running Process A and another rule for endpoints running Process B, both of which apply the "RP" tag to eligible endpoints.

ZTNA Access Proxies

You can deny or authorize a FortiGate in *ZTNA Access Proxies*. Authorized FortiGates synchronize endpoint and tagging data from EMS. FortiClient does not directly connect to FortiGates listed on this page.

To change the FortiGate authorization status:

1. Go to *Configuration* > *ZTNA Access Proxies*.
2. Select the desired FortiGate.
3. Click *Authorize* or *Disconnect*. The FortiGate status changes.

Domains

FortiSASE supports Active Directory (AD) domains, which work with these features:

- In *Configuration* > *Domains*, configuring FortiSASE Endpoint Management Service to connect to AD domains to allow viewing and selecting AD domains, users, and groups.
- Assigning endpoint profiles to AD-joined endpoints based on matching AD users or groups
- Zero trust network access tagging when these Windows rule types are configured and matching:
  - *User in AD Group*
  - *Domain*

For details on Entra ID domains, see Entra ID domains on page 263.

To configure an AD connection:

1. Go to *Configuration* > *Domain* and click *Create* > *Active Directory (AD) connection*.
2. Configure the AD server settings to match those on your AD server. Modify these to match your setup:

Field	Value
Name	Domain name from AD server
Server address	<AD server IP address or name>
Server Port	389
Username	administrator
Password	<Password>
Sync every	60 minutes
LDAPS connection	Disabled

3. Click *Authorize*. Upon success, observe the message *Connection to the Active Directory successfully authorized*.
4. Click *Sync*. You return to the *Configuration* > *Domains* page with a card with details about the newly added AD domain.

Entra ID domains

Supporting Entra ID domains only works with Windows endpoints running FortiClient 7.0.13 or later that are joined to Entra ID domains and are connected to the FortiSASE Endpoint Management Service.

FortiSASE supports Entra ID domains which work with these features:

- In *Configuration* > *Domains*, configuring FortiSASE Endpoint Management Service to connect to Entra ID domains to allow viewing and selecting Entra ID domains, users, and groups.
- Assigning endpoint profiles to Entra ID-joined endpoints based on matching Entra ID users or groups
- ZTNA tagging when these Windows rule types are configured and matching:
  - *User in AD Group*
  - *Domain*

Supporting Entra ID domains is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support.

Configuring API permissions and determining Entra ID SSO credentials

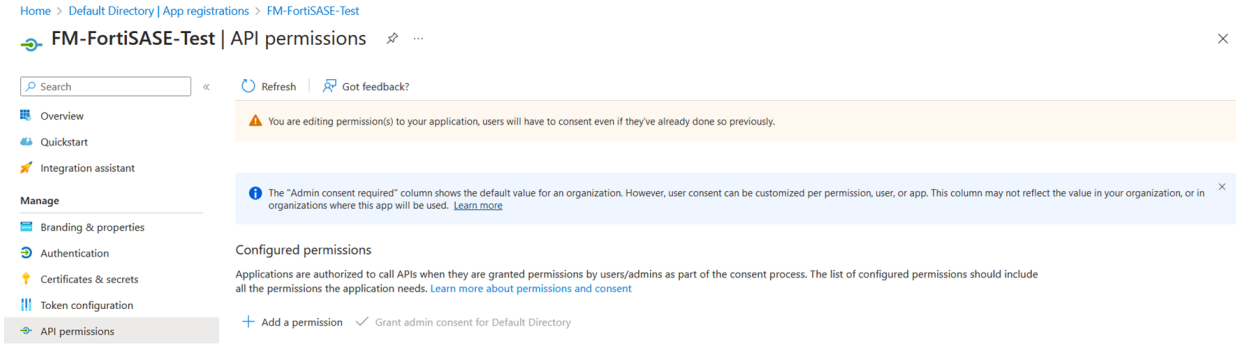
Before you can autoconnect to VPN using Microsoft Entra ID SSO and search user groups from Entra ID single sign on (SSO), you must configure API permissions for autoconnect and group searching, and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

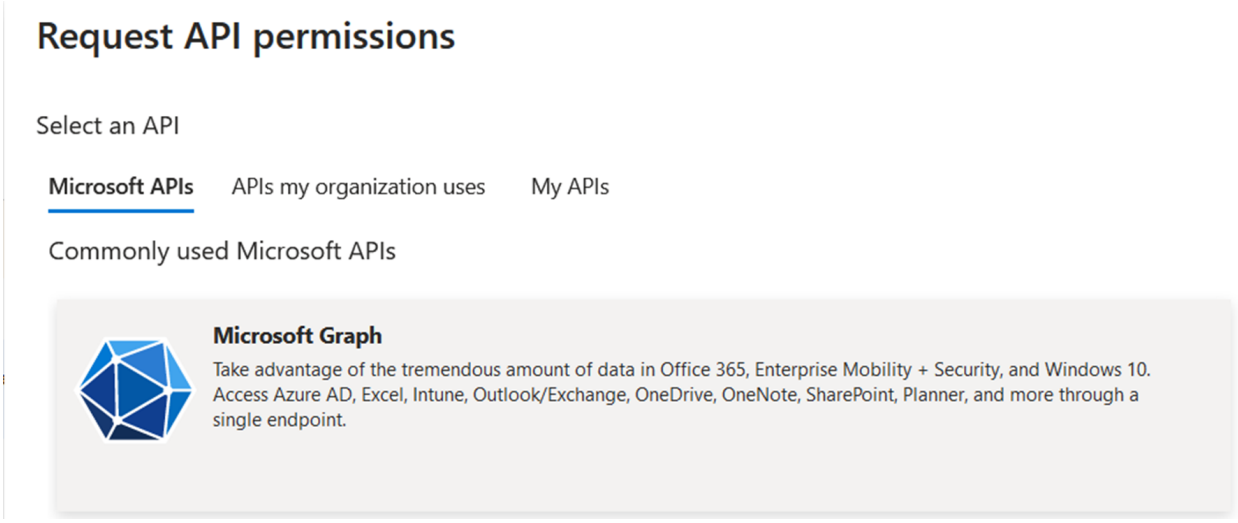
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information.
2. On the homepage, do one of the following:
   - Under *Azure Services*, click *Microsoft Entra ID*.
   - Click the navigation menu and under *All Services*, click *Microsoft Entra ID*.

To add Microsoft Graph API application permissions required for supporting an Entra ID domain:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.



4. In the *Request API permissions* slide-in, click *Microsoft Graph*.

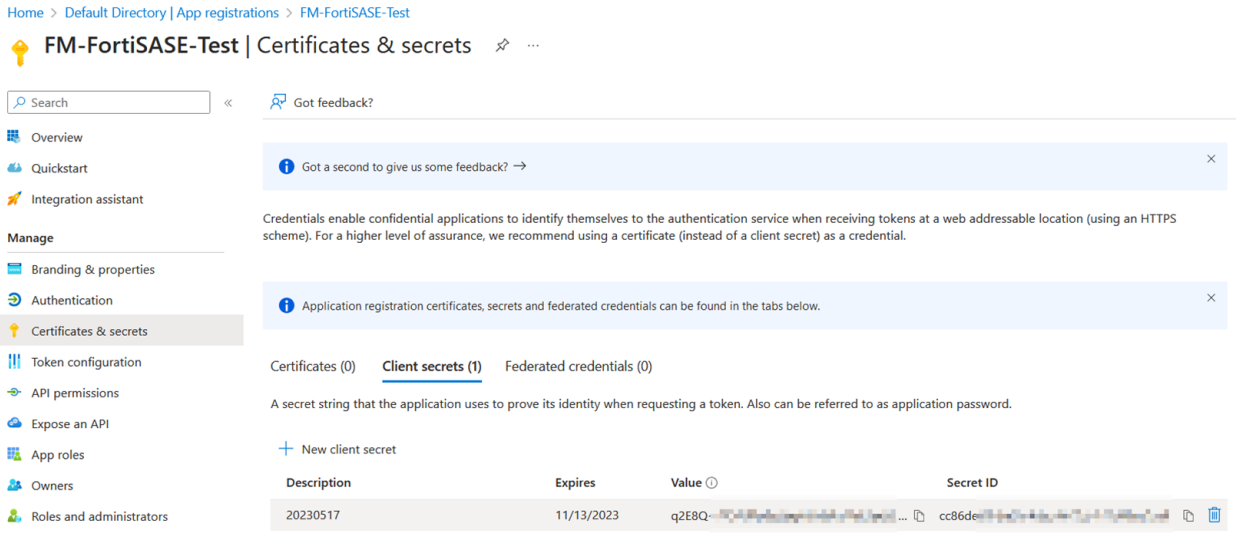


5. Add application permissions:
   a. Select *Application permissions*.
   b. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for group searching:
      - *Device > Device.Read.All – Read all devices*
      - *Domain > Domain.Read.All – Read domains*
      - *Group > Group.Read.All – Read all groups*
      - *GroupMember > GroupMember.Read.All – Read all group memberships*
      - *User > User.Read.All – Read all users' full profiles*
   c. Click *Add permissions*.
6. Add delegated permissions:
   a. Repeat steps 1-4 to add a permission.
   b. Select *Delegated permissions*.
   c. In the *Select permissions* section, search for and select the following permissions by clicking the checkboxes next to these permissions required for autoconnect:
      - *User > User.Read – Sign in and read user profile*
7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for <domain name>*. If this option is grayed out, you must log into an Entra ID admin account to perform this step. Click *Yes* in the *Grant admin consent* confirmation prompt. Observe the *Grant consent successful* notification at the top-right.
   Also, observe the *Status* field shows *Granted for <domain>* for all the permissions added.
   This step is important since it ensures that the administrator grants permissions for the enterprise application from Entra ID instead of end users requiring the administrator to log in to each instance and provide permissions.
   Therefore, in summary, you should add the following Microsoft Graph permissions to support the following Entra ID features:

Feature	API permission group	Permission name	Type
Entra ID domain support	*Device*	*Device.Read.All*	Application
	Domain	*Domain.Read.All*	
	Group	*Group.Read.All*	
	GroupMember	*GroupMember.Read.All*	
	User	*User.Read.All*	
		User.Read	Delegated

To add a client secret string and determine the value of the client secret string:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE enterprise application and click the hyperlinked name.
3. In the left menu, click *Certificates & secrets*, and click *New client secret*.
4. In the *Add a Client Secret* slide-in, add a *Description* and select the *Expires* option of your choice. Click *Add*.
5. Observe that a new client secret has been created. Immediately after creation, ensure you copy the *Value* of the client secret string, which FortiSASE uses as the *Client Secret*. This value is not visible after this initial creation step and moving to another page.



To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click *All applications*.
2. Look for your FortiSASE enterprise application name and click the hyperlinked name.
3. In the left menu, click *Overview* and note the following values:
   - *Application (client) ID*, which FortiSASE uses as the *Client ID*
   - *Directory (tenant) ID*, which FortiSASE uses as the *Tenant ID*

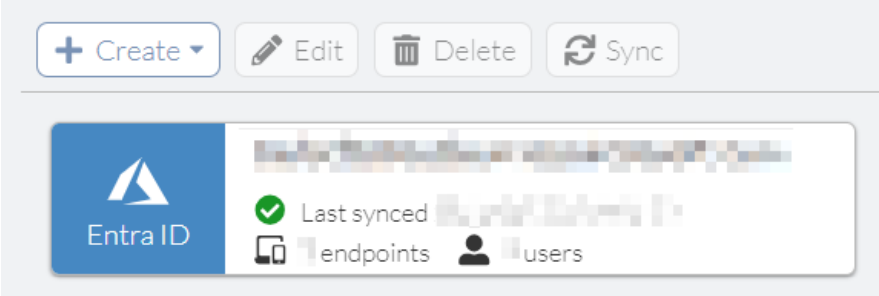
Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	*Directory (tenant) ID*	*Tenant ID*
	Application (client) ID	*Client ID*
Certificates & Secrets	*Value*	*Client Secret*

To configure an Entra ID connection:

1. Go to *Configuration* > *Domain* and click *Create* > *Entra ID connection*.
2. Configure the Entra ID domain settings to match those for your Entra ID tenant and application. Modify these to match your setup.

Field	Value
Name	Domain name from Entra ID
Tenant ID	*Directory (tenant) ID* from Entra ID
Client ID	*Application (client) ID* from Entra ID
Client secret	Value of *Client Secret* from Entra ID

3. Click *Authorize*. Upon success, observe the message *Connection to Entra ID successfully authorized. Click "Next" to synchronize groups*. Click *Next*.
4. Configure settings related to synchronizing groups:
5. Click *Sync*. You will return to the *Configuration* > *Domains* page with a card with details about the newly added AD domain.



6. To manually sync with Entra ID, select the card corresponding to the Entra ID domain and click *Sync*.

System

Certificates

You can upload a certificate for use with SSL deep inspection and LDAP and SAML single sign on (SSO) authentication.

To upload a certificate:

1. Go to *System* > *Certificates*.
2. Click *Import*, then do one of the following:
   - Select *Local Certificate* and configure the following:
     i. For *Type*, select *Local Certificate* to upload a custom service provider certificate in SSO configuration or *Local CA Certificate* to upload a custom SSL deep inspection certificate.
     ii. For *Format*, select *PKCS#12 Certificate* or *Certificate*.
     iii. In the *Certificate File* or *Certificate with Key File* field, click *Upload* to upload the certificate file. The certificate name is the same as the uploaded file name and can be a maximum of 35 characters long.
     iv. If you selected *Certificate* for *Format*, in the *Key File* field, click *Upload* to upload the key file.
     v. (Optional) Configure a password.
     vi. Click *OK*.
   - Select *Remote Certificate* and configure the following:
     i. For *Type*, select *Remote Certificate* to trust a remote server certificate public key. You can use this to upload an identity provider server certificate in SSO configuration. Select *Remote CA Certificate* to trust a remote server CA certificate. You can use this in LDAPS configuration.
     ii. Click *Upload* to upload the certificate file.
     iii. Enter a certificate name as desired. The certificate name can be a maximum of 35 characters long.
3. Click *OK*. The certificate displays in *System* > *Certificates*.

HTML Templates

You can customize block pages that display on endpoints in certain situations, such as if FortiSASE blocks access based on Application Control With Inline-CASB settings.

The following lists the HTML templates for block pages, email, and warning pages that you can customize in FortiSASE:

Name	Description
Block page	
Application Control Block page	Replacement HTML for Application Control With Inline-CASB block page
Banned Word Block Page	Replacement HTML for Banned Word/Content Web Filter block page
Data Loss Prevention Block	Replacement HTML for Data Loss Prevention block page

Name	Description
Page	
FortiGuard Block Page	Replacement HTML for FortiGuard Category Based Web Filter block page
URL Block Page	Replacement HTML for HTTP URL block page
Virus Block Page	Replacement HTML for AntiVirus block page
Virus Upload Block Page	Replacement HTML for virus infected file upload block page
Email	
Invitation Email	HTML email content for inviting users to FortiSASE
Warning Page	
FortiGuard Warning Page	Replacement HTML for FortiGuard Category Based Web Filter warning page

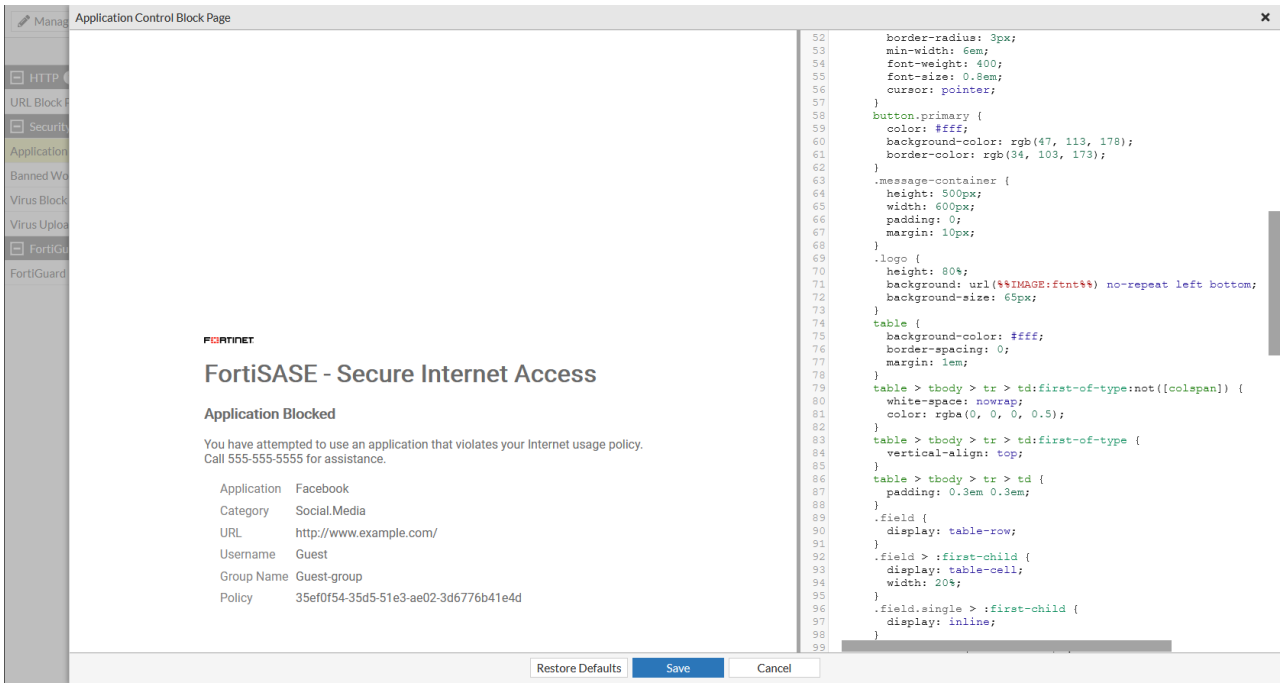
For example, you can customize the message to add your company logo and include your helpdesk phone number so that users can contact the network administrator about their machine. You can also customize the email to send to users to invite them to FortiSASE.

This example modifies the Application Control block page to use the Fortinet logo instead of the FortiSASE logo and include a phone number.

To customize the Application Control block page:

1. Go to *System* > *HTML Templates*.
2. On the *Images* tab, click *Create*.
3. In the *Name* field, enter the desired name. This example uses ftnt.
4. Upload the desired logo.
5. Click *OK*.
6. On the *Templates* tab, select *Application Control Block Page*, then click *Edit*.
7. To replace the FortiSASE logo, replace `%%IMAGE:logo_fortisase_sia&%% with %%IMAGE:<image name>%%`. This example replaces it with `%%IMAGE:ftnt%%`.
8. To add a phone number to the message, modify the `<body><div class="message-container"><p>You have attempted...</p>` element as desired.
9. Click *Save*. The endpoint user sees this page when they attempt to view an application that FortiSASE Application

Control With Inline-CASB blocks access to.



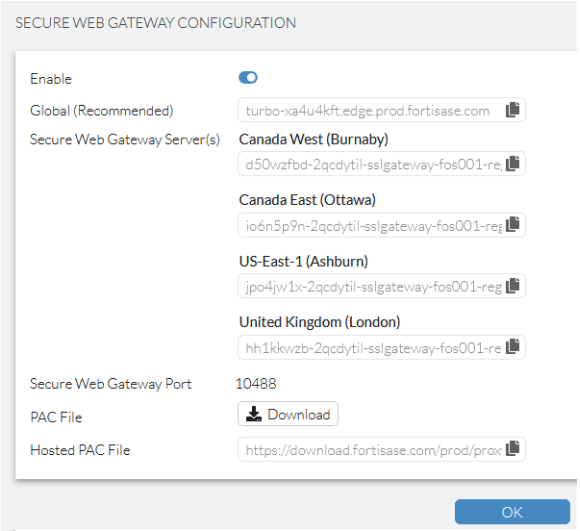
SWG Configuration

You can enable the secure web gateway (SWG) feature. When you enable the SWG feature, you can have end users configure their client software, such as a browser, to proxy all of its traffic through FortiSASE. You must manually send the SWG server information to end users. End users then configure their browser to send requests directly to the SWG.

To enable the SWG feature:

1. Go to *System* > *SWG Configuration*.
2. Toggle *Enable* to on. Click *OK*. The GUI may take a few minutes to reload. Once the GUI finishes loading, you can view the *Hosted PAC File* URL, which users use to configure the SWG server on their endpoints. You can also view

the default SWG policies and create custom ones in *Configuration* > *SWG Policies*. See SWG Policies on page 142.



Analytics

Under *Analytics*, you can generate reports and view logs. Reports and logs are useful components to help you understand what is happening on your network, and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.

Reports

You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, and manually run reports when desired.

Scheduling a report

To create an email group used for sending emails of scheduled reports:

1. Go to *Analytics* > *Scheduled Reports*.
2. Click *Manage email groups*.
3. Click *+Create*.
4. In the *New email group* slide-in, set the *Name*, *Subject*, *Body*, and *Description* accordingly. For *Recipients*, enter the email addresses that will receive the scheduled report that the email group will be configured with in the following steps.
5. Click *Close*.

To edit a report schedule:

1. Go to *Analytics* > *Scheduled Reports*.
2. Select the desired report. Click *Customize report* at the top and a slide-in window appears.
3. Set *Status* to *Enabled* to enable scheduling reports.
4. Set *Time period* to the desired time, indicating the timeframe from which FortiSASE uses logs to generate reports.
5. In the *Schedule* section, set the *Interval*, *Start time* (your local time), and optionally *End time* (your local time) for the report. FortiSASE generates the first report at the configured *Start time*. After the first generation, FortiSASE generates the report eternally at regular periods based on the configured *Interval* unless you configure an *End time*.
6. In *Output*, for *Send report to*, select the email group to send this report to.
7. Click *OK*.
8. When FortiSASE completes generating the report, view it in *Analytics* > *Generated Reports*.

Manually running a report

To manually run a report:

1. Go to *Analytics* > *Scheduled Reports*.
2. Select the desired report.
3. Click *Run Report* at the top.
4. When FortiSASE completes generating the report, view it in *Analytics* > *Generated Reports*.
5. You can download a report in PDF, HTML, XML, and CSV formats from *Analytics* > *Generated Reports*. Click the report and select the *Download* dropdown list to download it in the desired format.

Report types

Each report type has FortiSASE configuration dependencies that you must have configured in your FortiSASE instance to obtain valid data for the report.

You can view the configuration dependencies in *Analytics* > *Scheduled Reports* by following one of these steps:

- Scrolling to the right and viewing them in the *Dependencies* column
- Selecting the report, clicking *Customize report*, and viewing them in the *Dependencies* section under *Report*

For those reports with Application Control as a configuration dependency, application Control With Inline-CASB features are not guaranteed to work when other security features are disabled. Enabling one of the following security features is recommended: Antivirus, File filter, DLP, Web filter, or DNS filter.

The following lists the report types that you can generate in FortiSASE:

Title	Description
Application	
Application Risk and Control	Risks that applications introduce on endpoints and efforts to control those risks. The report organizes applications into categories and includes information such as high-risk application, high-risk application by bandwidth, web categories, vulnerability exploits, virus, botnet, adware malicious attacks, zero day, and file transfers.
Bandwidth and Applications Report	Traffic, bandwidth, and sessions that users and applications use on endpoints. Also includes a summary of destinations that the user and applications accessed.
Cyber-Bullying Indicators Report	Users exhibiting behavior that aligns with common cyberbullying indicators, such as use of offensive phrases on social media.
High Bandwidth Application Usage Report	Applications with high bandwidth usage that may affect network performance. This report focuses on the following application types: • Peer-to-peer, such as BitTorrent, Xunlei, Gnutella, and Filetopia • File sharing and storage applications, such as Onebox, Google Drive,

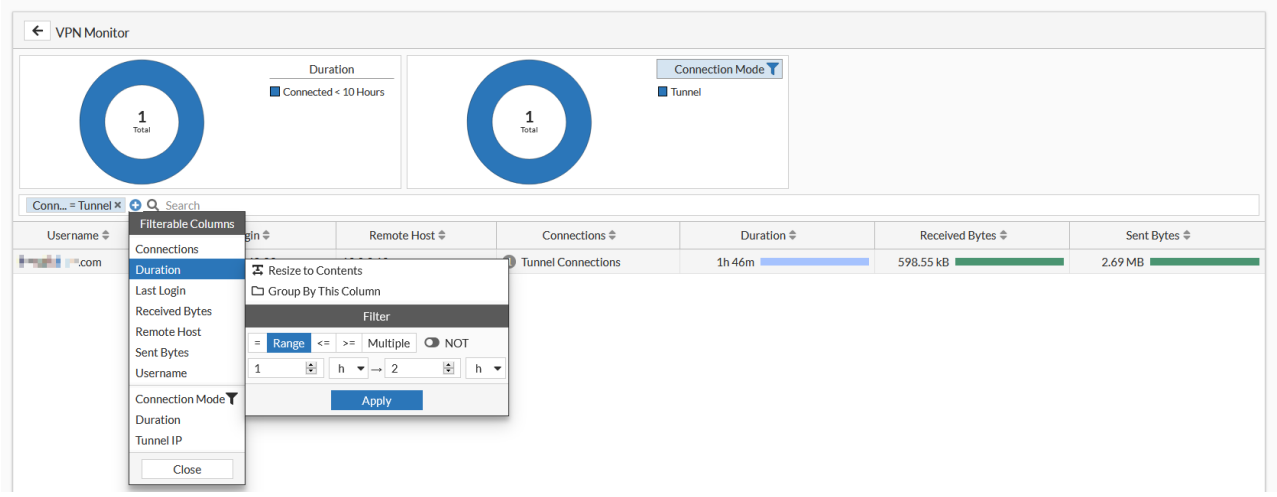
Title	Description
	Dropbox, and Apple Cloud • Voice or video applications, such as YouTube, Skype, Spotify, Vimeo, and Netflix
Self-Harm and Risk Indicators Report	Users exhibiting behavior that aligns with common self-harm and risk indicators, such as use of risky terms on social media.
Shadow IT Report	Summarizes the usage of SaaS apps compared to all applications, sanctioned vs unsanctioned SaaS applications, and total bandwidth by SaaS Sanctioned and Unsanctioned apps. Currently, this report does not support the Top 10 inline CASB applications by occurrences section.
Security	
Cyber Threat Assessment	Risk of applications on endpoints to cyber threats. Includes a review of application visibility and control, threat detection, threat prevention, and recommended actions.
Security Events and Incidents Summary	Security-related events or incidents that FortiSASE collected.
Threat Report	Malware and botnet attempts on endpoints. Includes detected malware and botnets. Also includes blocked intrusions, sources, and a timeline of the attempted intrusions as well as the blocked intrusion's severity rating.
VPN Report	VPN traffic on endpoints, including authenticated and failed user logins as well as top VPN users. Identifies remote VPN tunnels and users as well as web mode by bandwidth and duration.
Web Usage Summary Report	Web usage on endpoints and a bandwidth summary. Includes top active users and bandwidth usage. Also identifies users who are blocked the most from websites.

Logging

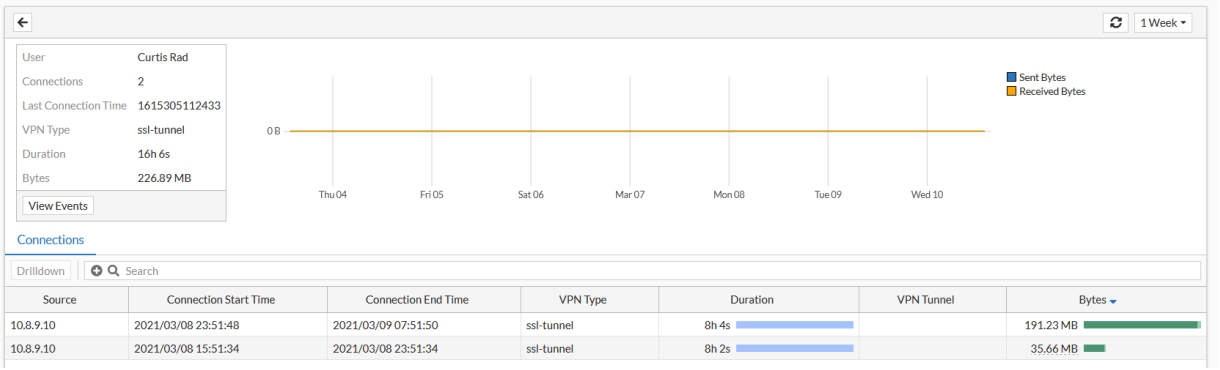
Logging and monitoring are useful components to help you understand what is happening on your network and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.

To find a connected user and drill down on logs:

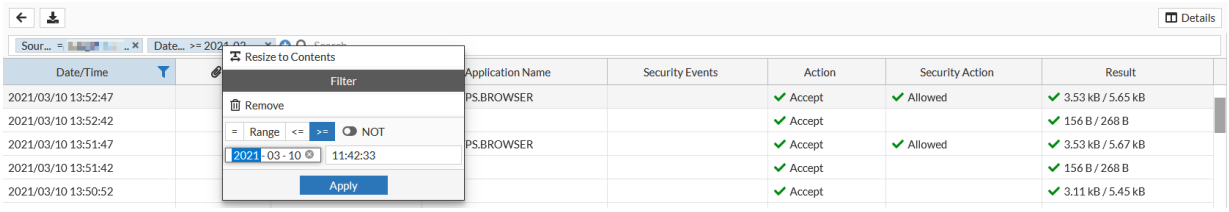
1. Go to *Dashboards* > *Users & Devices* > *VPN Monitor*.
2. The VPN Monitor displays currently connected VPN users. If desired, apply filters to the list of users displayed. For example, you can apply the *Duration* filter to only view users who have been connected for one to two hours:



3. Right-click the user that you want to drill down on. Select one of the following options:
   - *Show In FortiView*: goes to the *FortiView VPN* dashboard, which displays real-time VPN connection information for the selected user. To view historical data for the user, select *1 Day* or *1 Week* from the dropdown list in the top right corner.



   - *Show Matching Traffic Logs*: displays real-time traffic logs for the selected user. To view historical data for the user, select the applied *Date* filter. Apply a new filter for the desired timerange.



Forwarding logs to an external server

You can configure FortiSASE to forward logs to an external server, such as FortiAnalyzer.

To forward logs to an external server:

1. Go to *Analytics* > *Settings*.
2. Enable *Log Forwarding to Self-Managed Service*.
3. From *Remote Server Type*, select *FortiAnalyzer*, *Syslog*, or *Common Event Format (CEF)*.

4. For *Access Type*, configure the following:
   a. Select *Public* if the self-managed service is publicly accessible on the Internet.
   b. Select *Private* if the self-managed service is behind a Secure Private Access (SPA) FortiGate hub.
5. In the *Server Address* field and *Server Port* field (shown for *Syslog* and *CEF* types only), enter the desired address and port for FortiSASE to communicate with the server:
   a. If *Public* was selected for *Access Type*, then the *Server Address* field should be the public IP address or FQDN of the self-managed service.
   b. If *Private* was selected for *Access Type*, then the *Server Address* field should be the private IP address or FQDN of the self-managed service.
6. Enable *Reliable Connection* to use TCP for log forwarding instead of UDP.
7. For *Forwarding Frequency*, select *Real Time*, *Every Minute*, or *Every 5 Minutes* for log forwarding frequency from FortiSASE to the self-managed service.
8. Click *OK*.

To forward logs securely using TLS to an external syslog server:

1. Go to *Analytics* > *Settings*.
2. Enable *Log Forwarding*.
3. From *Remote Server Type*, select *Syslog*.
4. In the *Server Address* and *Server Port* fields, enter the desired address and port for FortiSASE to communicate with the syslog server.
5. Observe that *Reliable Connection* is enabled by default. Enabling this option enables TCP for log forwarding instead of UDP.
6. Observe that *Secure Connection* is enabled by default. Enabling this option enables TLS for log forwarding and requires *Reliable Connection* to be enabled.
   When hovering over the information icon, ensure the appropriate remote CA certificate for the external syslog server is uploaded for the TLS connection to succeed by clicking *Certificates*. Alternatively, go to *System* > *Certificates*.
   - For details on importing a remote CA certificate, see Certificates on page 268.
   - For details on the cipher suites that a secure external syslog server supports, see Supported cipher suites for secure external syslog server.

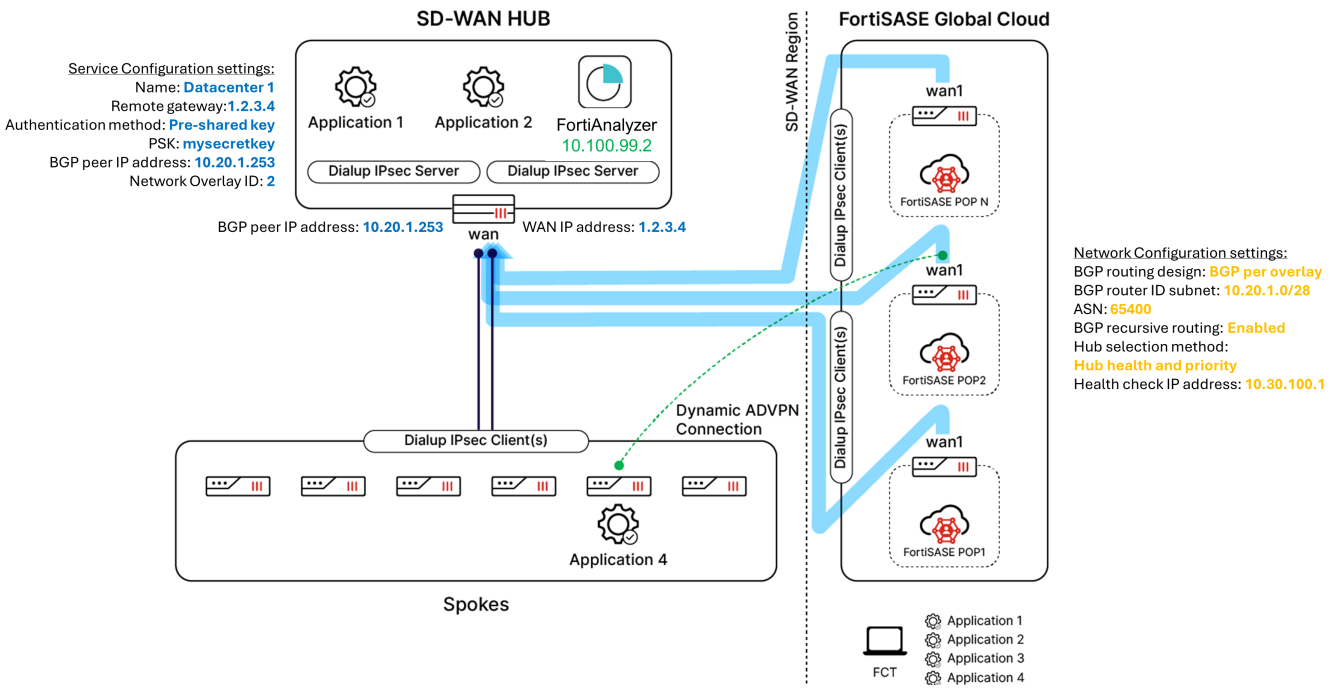
You must import the remote CA certificate for the external syslog server to FortiSASE to establish trust with the external syslog server. Otherwise, the TLS connection fails and the external syslog server cannot read the forwarded logs.

Example: Forwarding logs to an on-premise FortiAnalyzer in an SPA hub network

This example demonstrates how to configure forwarding logs to an on-premise FortiAnalyzer in an SPA hub network using the *Log Forwarding to Self-Managed Service* setting with the *Access Type* set to *Private*.

This example uses BGP per overlay as the BGP routing design because that is the default setting. The example also applies to the BGP on loopback BGP routing design.

In this example, we have the following SPA hub network topology using BGP per overlay as the BGP routing design:



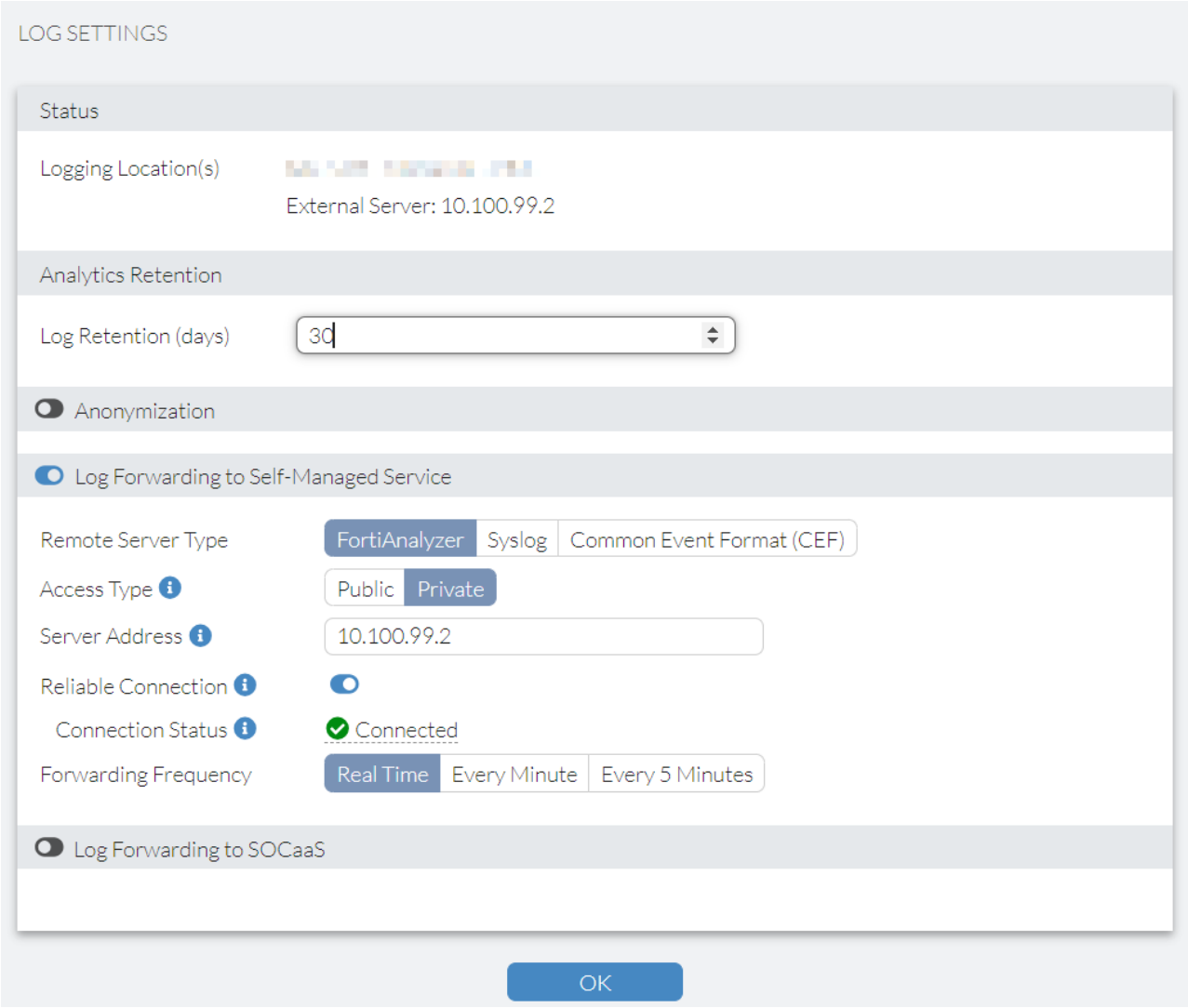
The FortiAnalyzer is in the SPA hub network with an IP address of 10.100.99.2.

For this example, you will configure FortiSASE to forward logs to the FortiAnalyzer using its private IP address on the SPA hub local network. Then you will authorize the FortiSASE PoPs on the FortiAnalyzer to allow FortiSASE to forward logs to the FortiAnalyzer. Lastly, you will verify that the logs from FortiSASE are forwarded to the FortiAnalyzer.

To configure forwarding logs to an on-premise FortiAnalyzer in an SPA hub network:

1. Go to *Analytics* > *Settings*.
2. Enable *Log Forwarding to Self-Managed Service*.
3. For *Remote Server Type*, select *FortiAnalyzer*.
4. For *Access Type*, select *Private* because the self-managed service (on-premise FortiAnalyzer) is behind a Secure Private Access (SPA) FortiGate hub.
5. In the *Server Address* field, enter 10.100.99.2, which is the private IP address of the self-managed service.
6. Enable *Reliable Connection* to use TCP for log forwarding instead of UDP.
7. For *Forwarding Frequency*, select *Real Time*.

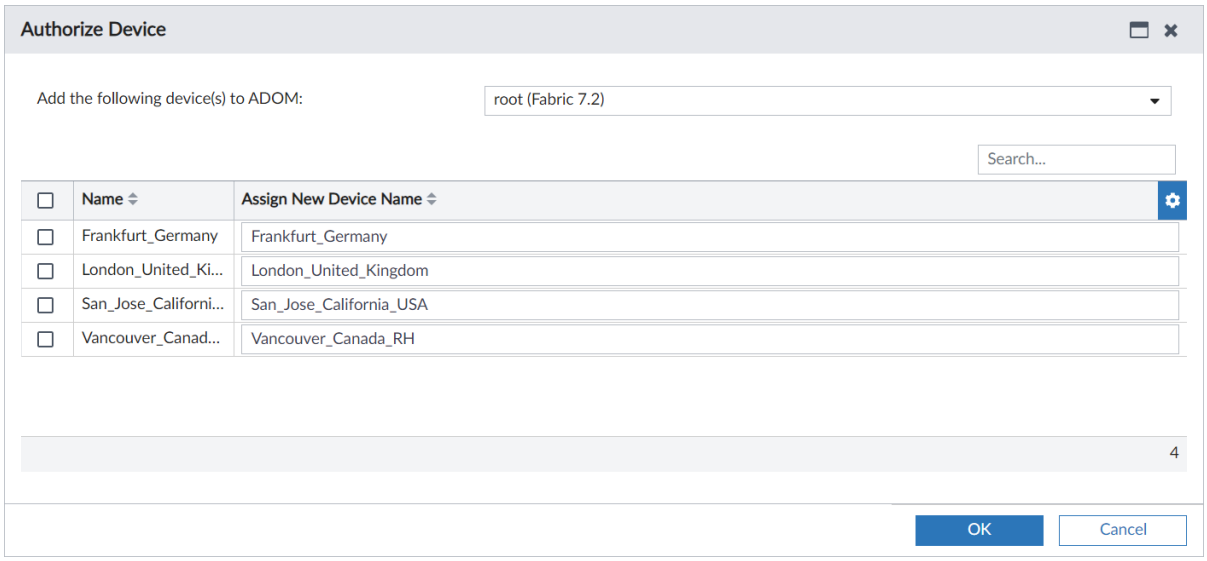
8. Click *OK*. After submitting the changes, the *Connection Status* changes from *Connecting* to *Connected*.



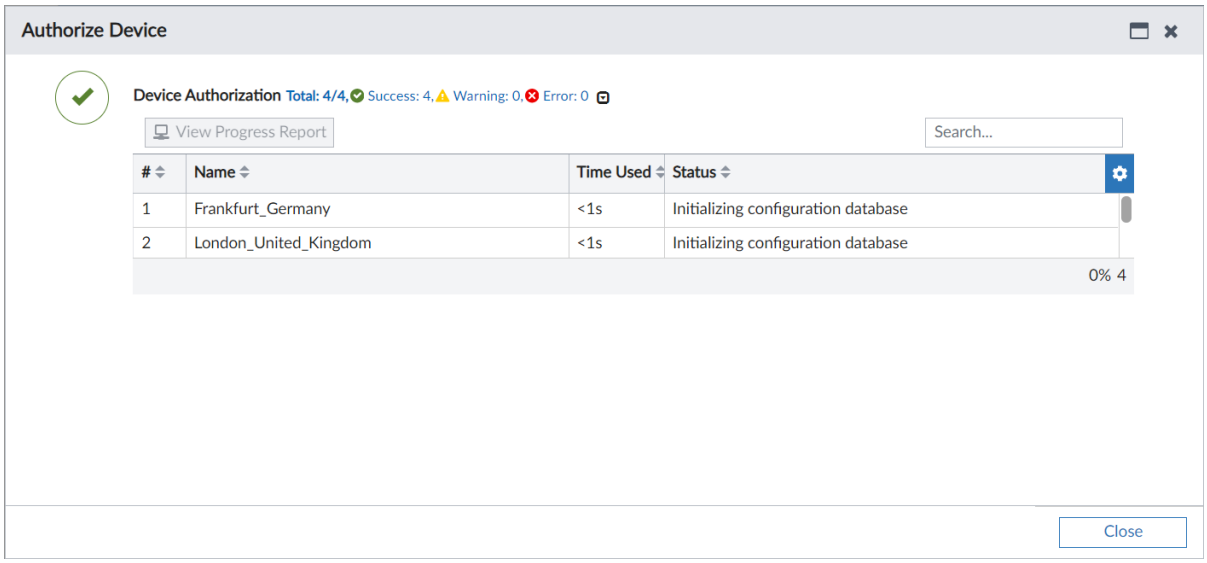
To authorize the FortiSASE PoPs on the FortiAnalyzer to allow FortiSASE to forward logs to the FortiAnalyzer:

1. Log on to the FortiAnalyzer GUI.
2. Go to the *Device Manager*.
3. In the *Device Manager*, under *Unauthorized Devices* observe the FortiSASE PoPs attempt to connect to FortiAnalyzer. Select all devices and click on *Authorize*.

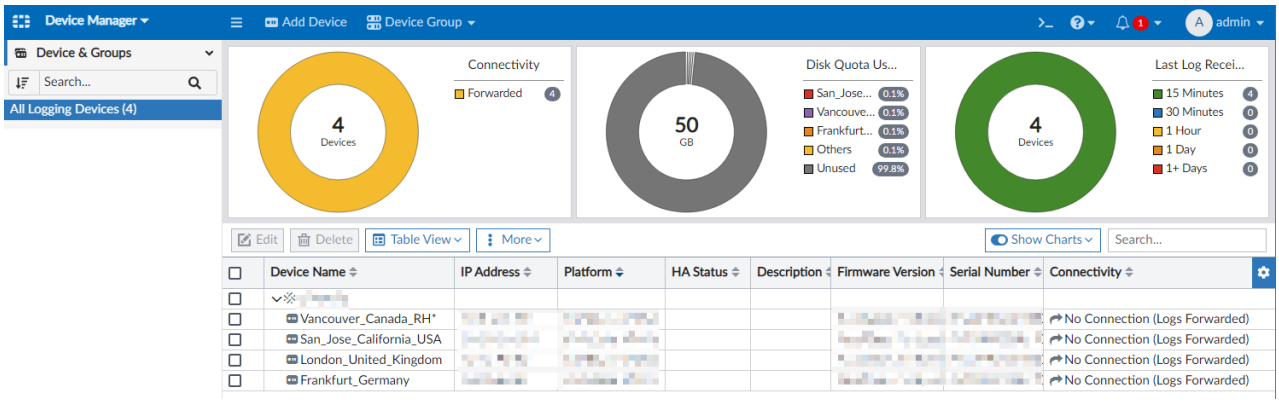
4. In the *Authorize Device* wizard, select all the devices, add them to the root ADOM, and click *OK*.



5. Observe *Device Authorization* succeeds for 4/4 devices. Click *Close*.

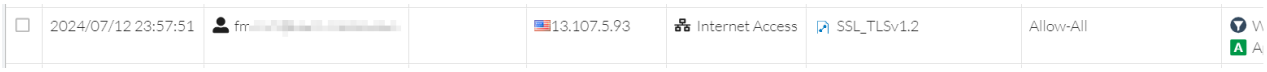


6. In the *Device Manager* page, wait for one minute and notice the *Connectivity* as *No Connection (Logs Forwarded)* as desired.



To verify that the logs from FortiSASE are forwarded to the FortiAnalyzer:

1. In FortiSASE, go to *Analytics* > *Traffic*.
2. Select *All Internet & Private Access Traffic*.
3. Observe one of the log entries with user fm to destination IP address 13.107.5.93:

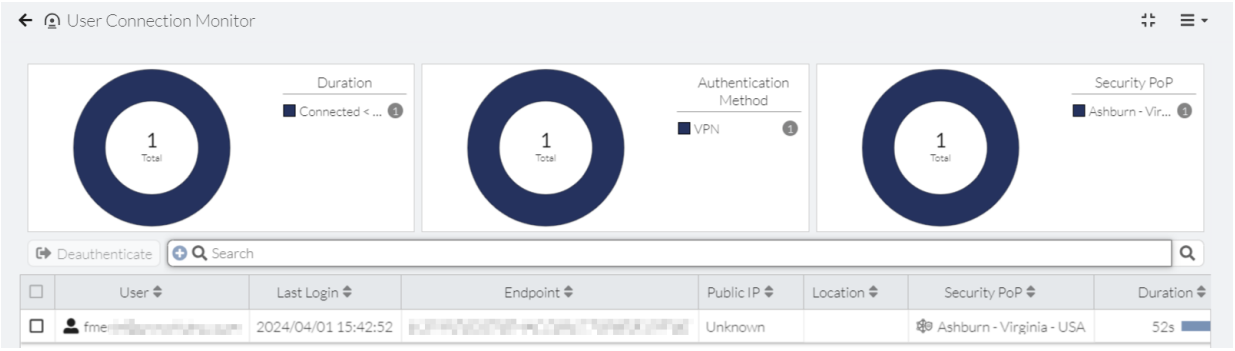


4. In FortiAnalyzer, go to *Log View*.
5. Go to *FortiGate* > *Traffic* to view the corresponding traffic log entries forwarded from FortiSASE.
6. In FortiAnalyzer, observe the log entry corresponding to the log entry observed in FortiSASE:

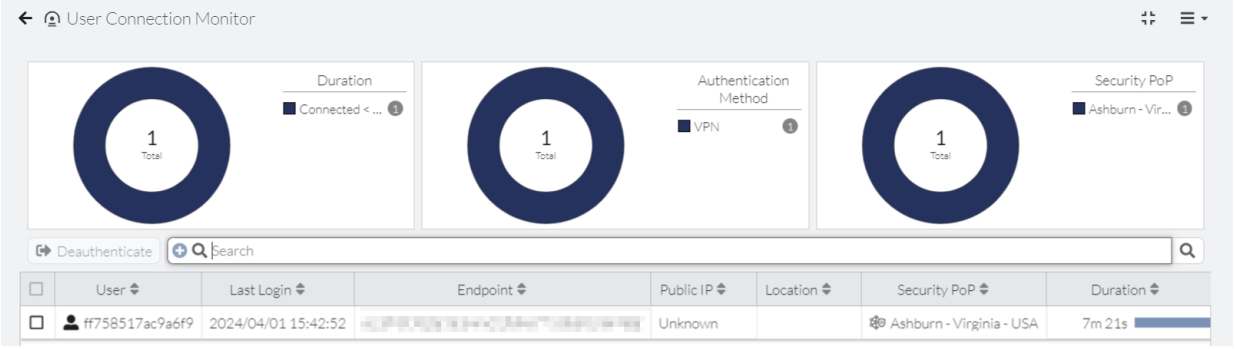
Log anonymization

Log anonymization allows you to hide personally identifiable user information, such as their username, in Dashboard widgets, logs, and other areas of FortiSASE.

The following shows the *Connected Users* page when log anonymization is disabled. The username information in the *User* field is visible.

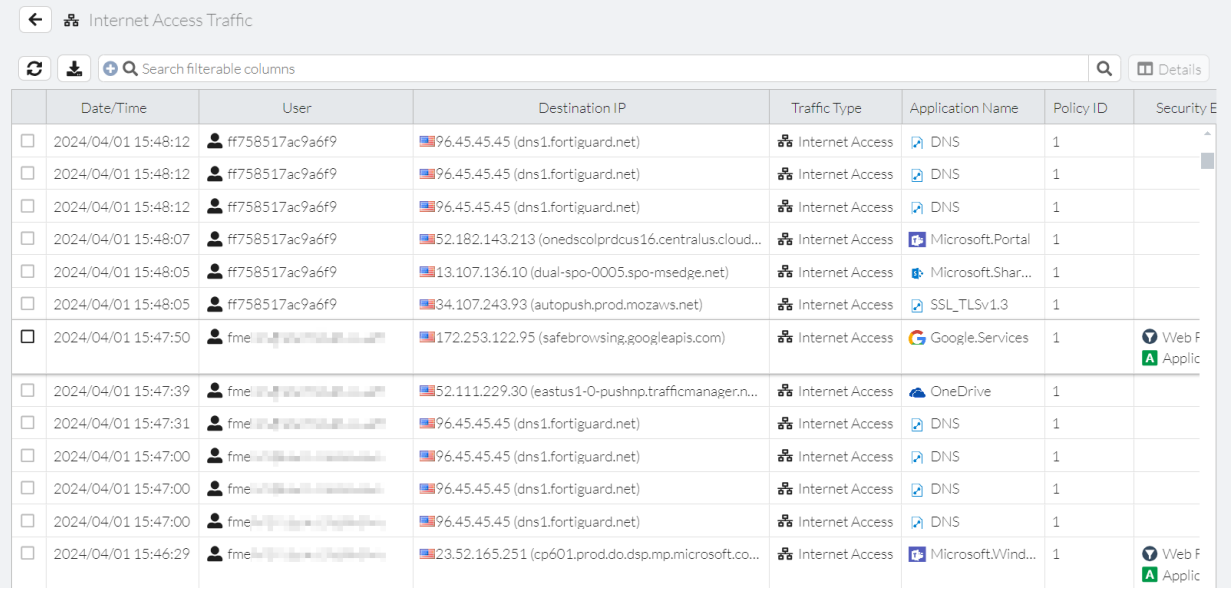


The following shows the *Connected Users* page when log anonymization is enabled. The username information in the *User* field is anonymized.

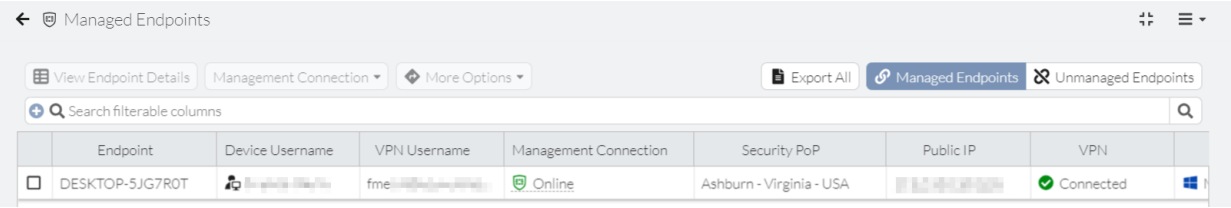


The following shows log anonymization's effect on *Analytics* > *Logs* > *Traffic*. In the following example, all logs are from the same source (user fme) and log anonymization was enabled at 15:48. All logs for traffic that occurred before 15:48 show the source information. All logs that occurred after 15:48 have the source information anonymized.

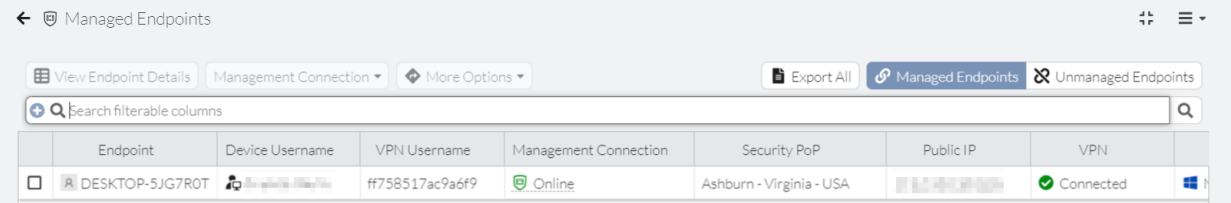
You cannot retroactively anonymize or deanonymize source information by enabling or disabling anonymization. The source information remains anonymized or not anonymized based on whether log anonymization was enabled or disabled when the traffic occurred.



The following shows the *Managed Endpoints* page when log anonymization is disabled. The username information is visible.



The following shows the *Managed Endpoints* page when log anonymization is enabled. The username is anonymized.



When log anonymization is enabled, reports may be less useful, as personally identifiable information will be anonymized.

To enable log anonymization:

1. Go to *Analytics* > *Settings*.
2. Enable *Anonymization*.

3. In the *Salt* field, enter the desired username anonymization hash salt. FortiSASE generates a hash based on the username and salt value and uses this to anonymize log information.

Administrator Events

Administrator Events logs under *Analytics* > *Events* provide granular logs that are useful to monitor and audit administrator activities such as login, MSSP portal access, configuration changes made by normal Identity & Access Management (IAM)/single sign on (SSO)/API user accounts or impersonated SSO/IAM accounts, contributing to effective auditing and compliance management. FortiSASE stores Administrator Events logs for the number of days that you specify in the log retention policy. See Log retention policy on page 282.

Currently, in FortiSASE, administrator event logs are displayed after some delay. Therefore, different timestamp fields are available for administrator events only to distinguish between the event's actual occurrence time and the time that the log was exported to FortiSASE.

Administrator Events log type	Timestamp field for actual event time (Unix timestamp in seconds)	Timestamp field for log export time to FortiSASE (Unix timestamp in nano-seconds)
FortiSASE Log Detail Window	Date/Time	Log Event Original Timestamp
Log forwarding to self-managed syslog or FortiSASE Downloaded Log File	audittime	eventtime
Log forwarding to self-managed FortiAnalyzer	Security Rating Time	Event Time

To view an Administrator Events log:

1. Go to *Analytics* > *Events*.
2. Click *Administrator Events*.
3. Double-click the desired log. A slide in window appears where you can view the log in detail.

Log retention policy

Log storage is fixed and log storage usage depends on factors such as number of users, number of policies with logging enabled, and logging type selected (security events, all sessions) for such policies. If log rotation occurs ahead of the configured log retention period, open a FortiCare support ticket to request a log storage increase for your instance.

You can configure FortiSASE to store logs up to a certain number of days that you specify as the log retention policy. FortiSASE automatically deletes logs that are older than the specified log retention (days).

All FortiSASE instances have log retention enabled with a log retention period of 30 days by default. You can configure the log retention policy to between 2 to 30 days. The policy applies to traffic, security, and event logs.

To store logs for a longer duration, configuring log forwarding to an external server is advised. See Forwarding logs to an external server on page 275.

To configure log retention policy:

1. Go to *Analytics* > *Settings*.
2. Enable the *Analytics Retention* toggle and set the *Log Retention (days)* to the required number of days.
3. Click *OK* to save the changes.

Forwarding logs to SOCaaS

To provide integration with FortiGuard SOC-as-a-Service (SOCaaS), FortiSASE supports the ability to configure log forwarding from FortiSASE to a SOCaaS collector using *Log Forwarding to SOCaaS* in *Analytics* > *Settings*.

To be configurable, *Log Forwarding to SOCaaS* requires an Advanced remote users FortiSASE license or a Comprehensive remote users FortiSASE license. Otherwise, FortiSASE grays out this option in *Analytics* > *Settings*. See the FortiSASE Ordering Guide.

To configure log forwarding to SOCaaS:

1. Go to *Analytics* > *Settings*.
2. Enable *Log Forwarding to SOCaaS*.
3. Click *OK*.
4. Once FortiSASE enables this feature, observe the following:
   a. A prompt instructs you to *Start Onboarding*. If you click *Start Onboarding*, a browser window opens for the SOCaaS portal to complete onboarding. Once you complete onboarding, FortiSASE sends a service request to the SOCaaS team. Completing onboarding on the SOCaaS portal is important for this feature to work as intended.
   b. In *Status*, *Logging Location(s)* displays a *SOCaaS Collector Region*.
   c. Under *Log Forwarding to SOCaaS*, *Connection Status* displays *Connected* with a green checkmark. Hovering over the *Connection Status* value shows the rate at which FortiSASE forwards logs.

Currently, you cannot disable the *Log Forwarding to SOCaaS* feature from *Analytics* > *Settings* once you have enabled it because the toggle is grayed out. To disable this feature, you must create a new FortiCare ticket.

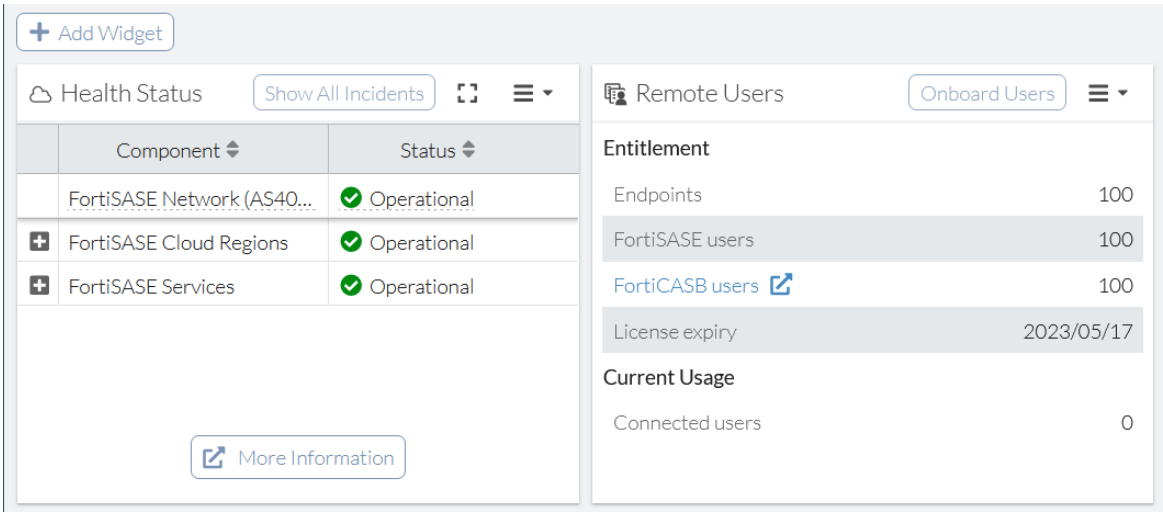
Client onboarding

Clients using managed endpoints connect using VPN. You can onboard them using the *Onboard Users* slide-in.

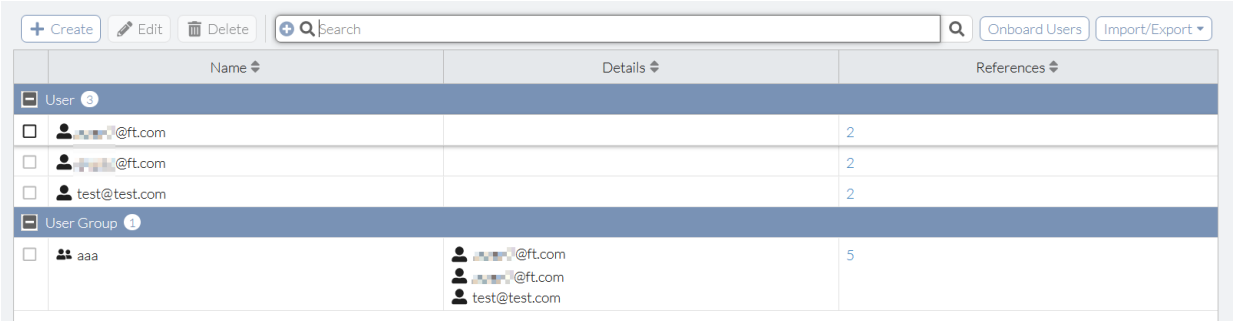
To access the Onboard Users slide-in:

You can access the *Onboard Users* page by doing one of the following:

- Go to *Dashboard* > *Status* and under the *Remote Users* widget, click *Onboard Users*. If this widget does not exist, add a new *Remote Users* widget as Adding a custom dashboard on page 26 describes.



- Go to *Configuration* > *Users* and click *Onboard Users* at the top right of the page.



When you click the *Onboard Users* button, the *Onboard Users* slide-in page appears. The page consists of the following sections:

- Managed Endpoint Users. See Managed endpoint client onboarding on page 285.
- Secure Web Gateway Users. See SWG client onboarding on page 286.

Managed endpoint client onboarding

For instances with the Advanced or Comprehensive remote user license and Windows endpoints, the MSI version of the FortiClient installer does not install the Digital Experience Monitoring (DEM) agent on the endpoint. You must use the executable version of the FortiClient installer to install the DEM agent on Windows endpoints.

Onboard Users > *Managed Endpoint Users* includes features to support onboarding managed endpoint clients.

Feature	Description
FortiClient Version	Recommended FortiClient version for FortiSASE users.

FortiClient Installer	Method for obtaining the FortiClient installer:
	• *Download*: download the installer directly from the FortiSASE portal. The remaining features in this table appear when you select this method.
	• *Send link to users*: send invitation email to selected users containing links to FortiClient installers for all major operating systems (OS). When you select this method, the following options appear:
	  • *Installer Type*:
	  • *Pre-configured*: installer is preconfigured to connect with FortiSASE, that is, the invitation code is built-in.
	  • *Manual*: after downloading and launching the installer, users must manually enter the invitation code sent in the email.
	  • *Invite Users*: click + to add a blank field where you can enter a managed endpoint user's email address to onboard to FortiSASE. Click + as many times as desired to enter multiple email addresses. When you complete entering managed endpoint users' email addresses, click *Send*.

Preconfigured installer	
OS	Use the *OS* dropdown to select the installer for the major OS that you want to download. These installers are preconfigured with your FortiSASE invitation code.
Download Installer	After selecting an OS, clicking *Download Installer* downloads the preconfigured installer for the selected OS to your local machine.
Manual Installer	
Invitation Code	After downloading and launching the FortiClient installer, this is the code to input into FortiClient to allow managed users to be automatically provisioned to connect to FortiSASE. In FortiClient, on the *Zero Trust Telemetry* tab, input the invitation code from FortiSASE in the *Register with Zero Trust Fabric* field, and click *Connect*.
OS	Use the *OS* dropdown to select the installer for the major OS that you want to download. These installers are not preconfigured with your FortiSASE invitation code.

Feature	Description
Download Installer	After selecting an OS, clicking *Download Installer* downloads the preconfigured installer for the selected OS to your local machine.
Generic FortiClient Installers	These installers are publicly available installers that do not come preconfigured with your FortiSASE invitation code. Clicking a generic installer for a supported OS goes to a download page where you can select and download the installer to your local machine.

For the *Preconfigured Installer* or *Manual Installer*, you can proceed to provision your endpoints by doing one of the following:

- Using a mobile device management (MDM) software suite using the installer
- Distributing the installer to end users and having them install it on their endpoints

When using the *Manual Installer*, whether you decide to provision your endpoints using this installer and an MDM, or distribute this installer to end users, end users must still input the invitation code that you provide for your FortiSASE instance.

SWG client onboarding

PAC file customization

FortiSASE secure web gateway (SWG) mode involves configuring and hosting a proxy autoconfiguration (PAC) file for respective endpoints to connect to the FortiSASE gateway.

A PAC file is based on JavaScript and contains rules for the proxy client to follow to route traffic to the proxy server or directly to the internet. For FortiSASE SWG users:

- The proxy client is a web browser or another proxy-aware application.
- The proxy server is the FortiSASE SWG.
- Routing traffic to the proxy uses the FortiSASE SWG as a web proxy.
- Routing traffic directly to the internet bypasses the FortiSASE SWG.

Typically, some web applications require traffic to be routed directly to the internet for specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly. In these cases, you must customize the PAC file with specific IP addresses and hostnames, and then host the custom PAC file on a server that the endpoints can access.

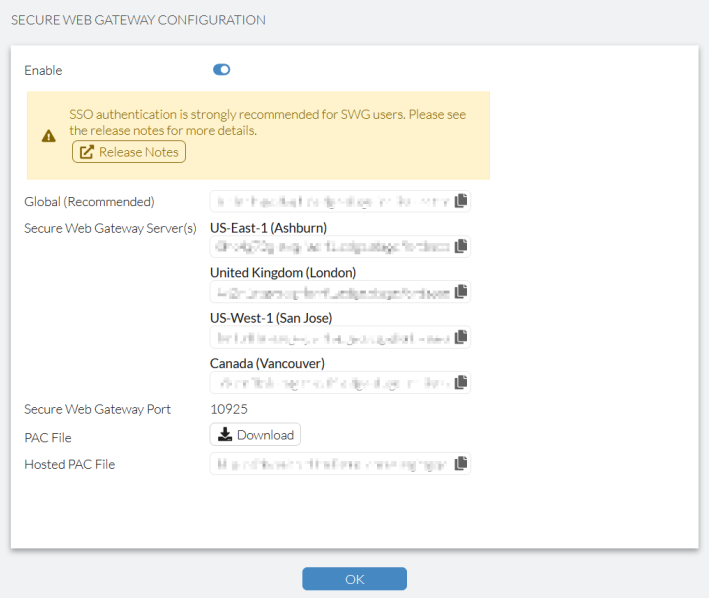
The workflow for customizing and using a PAC file is as follows:

1. FortiSASE provides a preconfigured PAC file hosted on the FortiSASE server for use. Download the PAC file to a computer for editing.
2. Customize the PAC file in a text editor to exclude certain hosts from being proxied.
3. Host the custom PAC file on a server accessible by the endpoints.
4. On an endpoint, download and install the SWG certificates provided in the FortiSASE portal.
5. On an endpoint, install and configure the client browser or OS settings to point to the hosted custom PAC file.

While setting up SSO with AD FS or other custom identity providers (IdP) (except Google, Entra ID, FortiTrustID, or Okta) for agentless users, customizing the PAC file to add IdP URLs to it such that the traffic to IdP URLs is not forwarded to the FortiSASE secure web gateway (SWG) server and instead goes directly to the internet is mandatory. See Customizing the PAC file on page 287.

Downloading the preconfigured PAC file

The *System* > *SWG Configuration* page displays the secure web gateway (SWG) servers, port, and hosted proxy autoconfiguration (PAC) file. You can download the predefined PAC file to customize.



By default, the FortiSASE hosted PAC file contains the global (recommended) URL and the SWG port specific to your instance. This global (recommended) URL automatically directs users to the closest geographical location for all browsers and proxy-aware applications. For example:

```
function FindProxyForURL(url, host) {
    return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
}
```

This simple PAC file specifies that the web request should be sent through the proxy server turbo-hqwdvq17.edge.prod.fortisase.com on TCP port 10925 and if the proxy does not respond to this request, the browser sends the web request directly to the internet without using the proxy.

Customizing the PAC file

This example customizes the PAC file to exclude common external URLs and networks from being forwarded to the FortiSASE secure web gateway (SWG) server, which allows specific domains which do not support redirection for security reasons or are required for authentication, such as common SAML identity providers, to load correctly.

You must replace the final `return` statement at the end of the PAC file with the corresponding proxy URL and port listed in your preconfigured PAC file in the previous step Downloading the preconfigured PAC file on page 287.

```
function FindProxyForURL(url, host) {
// Apple
if (dnsDomainIs (host, "albert.apple.com") ||
       dnsDomainIs (host, "captive.apple.com") ||
       dnsDomainIs (host, "gs.apple.com") ||
       dnsDomainIs (host, "humb.apple.com") ||
       dnsDomainIs (host, "static.ips.apple.com") ||
       dnsDomainIs (host, "sq-device.apple.com") ||
       dnsDomainIs (host, "tbsc.apple.com") ||
       shExpMatch (host, "*.push.apple.com") ||
       dnsDomainIs (host, "deviceenrollment.apple.com") ||
       dnsDomainIs (host, "deviceservices-external.apple.com") ||
       dnsDomainIs (host, "gdmf.apple.com") ||
       dnsDomainIs (host, "identity.apple.com") ||
       dnsDomainIs (host, "iprofiles.apple.com") ||
       dnsDomainIs (host, "mdmenrollment.apple.com") ||
       dnsDomainIs (host, "setup.icloud.com") ||
       dnsDomainIs (host, "vpp.itunes.apple.com") ||
       shExpMatch (host, "*.business.apple.com") ||
       shExpMatch (host, "*.school.apple.com") ||
       dnsDomainIs (host, "upload.appleschoolcontent.com") ||
       dnsDomainIs (host, "ws-ee-maidsvc.icloud.com") ||
       dnsDomainIs (host, "axm-adm-enroll.apple.com") ||
       dnsDomainIs (host, "axm-adm-mdm.apple.com") ||
       dnsDomainIs (host, "axm-adm-scep.apple.com") ||
       dnsDomainIs (host, "axm-app.apple.com") ||
       dnsDomainIs (host, "appldnld.apple.com") ||
       dnsDomainIs (host, "configuration.apple.com") ||
       dnsDomainIs (host, "gdmf.apple.com") ||
       dnsDomainIs (host, "gg.apple.com") ||
       dnsDomainIs (host, "gnf-mdn.apple.com") ||
       dnsDomainIs (host, "gnf-mr.apple.com") ||
       dnsDomainIs (host, "gs.apple.com") ||
       dnsDomainIs (host, "ig.apple.com") ||
       dnsDomainIs (host, "mesu.apple.com") ||
       dnsDomainIs (host, "ns.itunes.apple.com") ||
       dnsDomainIs (host, "oscdn.apple.com") ||
       dnsDomainIs (host, "osrecovery.apple.com") ||
       dnsDomainIs (host, "skl.apple.com") ||
       dnsDomainIs (host, "swcdn.apple.com") ||
       dnsDomainIs (host, "swdist.apple.com") ||
       dnsDomainIs (host, "swdownload.apple.com") ||
       dnsDomainIs (host, "swscan.apple.com") ||
       dnsDomainIs (host, "updates-http.cdn-apple.com") ||
       dnsDomainIs (host, "updates.cdn-apple.com") ||
       dnsDomainIs (host, "xp.apple.com") ||
       shExpMatch (host, "*.itunes.apple.com") ||
       shExpMatch (host, "*.apps.apple.com") ||
       shExpMatch (host, "*.mzstatic.com") ||
       dnsDomainIs (host, "itunes.apple.com") ||
       dnsDomainIs (host, "ppq.apple.com") ||
       dnsDomainIs (host, "appldnld.apple.com") ||
       dnsDomainIs (host, "appldnld.apple.com.edgesuite.net") ||
       dnsDomainIs (host, "itunes.com") ||
       dnsDomainIs (host, "itunes.apple.com") ||
       dnsDomainIs (host, "updates-http.cdn-apple.com") ||
```

```
        dnsDomainIs (host, "updates.cdn-apple.com") ||
        dnsDomainIs (host, "lcdn-registration.apple.com") ||
        dnsDomainIs (host, "suconfig.apple.com") ||
        dnsDomainIs (host, "xp-cdn.apple.com") ||
        dnsDomainIs (host, "lcdn-locator.apple.com") ||
        dnsDomainIs (host, "serverstatus.apple.com") ||
        dnsDomainIs (host, "17.248.128.0/18") ||
        dnsDomainIs (host, "17.250.64.0/18") ||
        dnsDomainIs (host, "17.248.192.0/19") ||
        shExpMatch (host, "*.appattest.apple.com") ||
        dnsDomainIs (host, "bpapi.apple.com") ||
        dnsDomainIs (host, "cssubmissions.apple.com") ||
        dnsDomainIs (host, "fba.apple.com") ||
        dnsDomainIs (host, "diagassets.apple.com") ||
        dnsDomainIs (host, "doh.dns.apple.com") ||
        dnsDomainIs (host, "certs.apple.com") ||
        dnsDomainIs (host, "crl.apple.com") ||
        dnsDomainIs (host, "crl.entrust.net") ||
        dnsDomainIs (host, "crl3.digicert.com") ||
        dnsDomainIs (host, "crl4.digicert.com") ||
        dnsDomainIs (host, "ocsp.apple.com") ||
        dnsDomainIs (host, "ocsp.digicert.cn") ||
        dnsDomainIs (host, "ocsp.digicert.com") ||
        dnsDomainIs (host, "ocsp.entrust.net") ||
        dnsDomainIs (host, "ocsp2.apple.com") ||
        dnsDomainIs (host, "valid.apple.com") ||
        dnsDomainIs (host, "appleid.apple.com") ||
        dnsDomainIs (host, "appleid.cdn-apple.com") ||
        dnsDomainIs (host, "idmsa.apple.com") ||
        dnsDomainIs (host, "gsa.apple.com") ||
        shExpMatch (host, "*.apple-cloudkit.com") ||
        shExpMatch (host, "*.apple-livephotoskit.com") ||
        shExpMatch (host, "*.apzones.com") ||
        shExpMatch (host, "*.cdn-apple.com") ||
        shExpMatch (host, "*.gc.apple.com") ||
        shExpMatch (host, "*.icloud.com") ||
        shExpMatch (host, "*.icloud.com.cn") ||
        shExpMatch (host, "*.icloud.apple.com") ||
        shExpMatch (host, "*.icloud-content.com") ||
        shExpMatch (host, "*.iwork.apple.com") ||
        dnsDomainIs (host, "mask.icloud.com") ||
        dnsDomainIs (host, "mask-h2.icloud.com") ||
        dnsDomainIs (host, "mask-api.icloud.com") ||
        dnsDomainIs (host, "audiocontentdownload.apple.com") ||
        dnsDomainIs (host, "devimages-cdn.apple.com") ||
        dnsDomainIs (host, "download.developer.apple.com") ||
        dnsDomainIs (host, "playgrounds-assets-cdn.apple.com") ||
        dnsDomainIs (host, "playgroups-cdn.apple.com") ||
        dnsDomainIs (host, "sylvan.apple.com"))
    return "DIRECT";

// VMWare
if (shExpMatch (host, "*.awmdm.com"))
    return "DIRECT";

// Okta
```

```
if (shExpMatch (host, "*.okta.com") ||
    shExpMatch (host, "*.oktacdn.com"))
    return "DIRECT";

// Microsoft
if (dnsDomainIs (host, "login.microsoftonline.com") ||
       shExpMatch (host, "*.officeconfig.msocdn.com") ||
       dnsDomainIs (host, "config.office.com") ||
       dnsDomainIs (host, "graph.windows.net") ||
       dnsDomainIs (host, "enterpriseregistration.windows.net") ||
       shExpMatch (host, "*.manage.microsoft.com") ||
       dnsDomainIs (host, "manage.microsoft.com") ||
    shExpMatch (host, "*.microsoftonline.com") ||
    shExpMatch (host, "*.msauth.net"))
    return "DIRECT";

// Google
if (dnsDomainIs (host, "client1.google.com") ||
    dnsDomainIs (host, "client2.google.com") ||
    dnsDomainIs (host, "client3.google.com") ||
    dnsDomainIs (host, "client4.google.com") ||
    dnsDomainIs (host, "client5.google.com") ||
    dnsDomainIs (host, "client6.google.com") ||
    dnsDomainIs (host, "chrome.google.com") ||
    dnsDomainIs (host, "commondatastorage.googleapis.com") ||
    dnsDomainIs (host, "dl-ssl.google.com") ||
    dnsDomainIs (host, "dl.google.com") ||
    dnsDomainIs (host, "gweb-gettingstartedguide.appspot.com") ||
    dnsDomainIs (host, "m.google.com") ||
    dnsDomainIs (host, "hangouts.google.com") ||
    dnsDomainIs (host, "pack.google.com") ||
    dnsDomainIs (host, "safebrowsing-cache.google.com") ||
    dnsDomainIs (host, "safebrowsing.google.com") ||
    dnsDomainIs (host, "ssl.gstatic.com") ||
    dnsDomainIs (host, "storage.googleapis.com") ||
    dnsDomainIs (host, "tools.google.com") ||
    dnsDomainIs (host, "www.googleapis.com") ||
    shExpMatch (host, "*.gstatic.com") ||
    dnsDomainIs (host, "play.google.com") ||
    dnsDomainIs (host, "mtalk.google.com") ||
    dnsDomainIs (host, "accounts.google.com") ||
    dnsDomainIs (host, "aadcdn.msftauthimages.net") ||
    dnsDomainIs (host, "aadcdn.msftauth.net") ||
    dnsDomainIs (host, "omahaproxy.appspot.com") ||
    dnsDomainIs (host, "cros-omahaproxy.appspot.com"))
    return "DIRECT";

// Replace this line with the corresponding line from your FortiSASE deployment's
preconfigured PAC file
return "PROXY turbo-hqwdvq17.edge.prod.fortisase.com:10925; DIRECT";
}
```

To selectively use sections of exempted URLs above, you can comment them out using the double slash `//` at the beginning of each JavaScript line to prevent the URLs from being exempted and force them to go through the FortiSASE SWG.

For example, to ensure VMware Workspace One traffic is sent to the proxy, since the rule consists of an *if* statement and a return statement, comment them out both:

```
// VMWare
// if (shExpMatch (host, "*.awmdm.com"))
//    return "DIRECT";
```

Hosting the custom PAC file

Once you have modified the proxy autoconfiguration (PAC) file, you should host it on a web server (such as Amazon S3) that is externally accessible by your remote users. The web server must be configured to allow .PAC file extensions to be downloaded and specified using the MIME type application/x-ns-proxy-autoconfig.

The PAC file does not require user authentication to access. However, any user that is pointing to the PAC file will be subject to authentication by FortiSASE when it accesses the internet.

Additional endpoint configuration steps

To complete the workflow for using a custom PAC file, the end user must download and install the SWG certificate on the endpoint and point the endpoint's web browsers to this hosted PAC file.

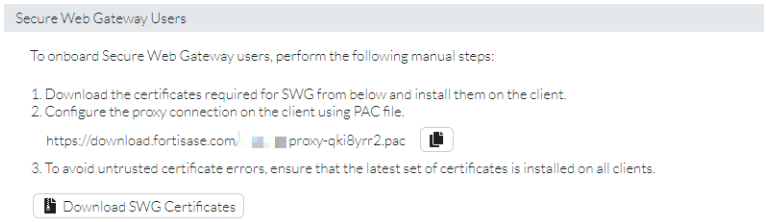
For details on downloading and installing the SWG certificate on an endpoint, refer to the steps in Certificate installation on page 291.

For details on configuring the endpoint to use the custom hosted PAC file, refer to the steps in Proxy configuration on page 292.

Certificate installation

When users connect to FortiSASE in secure web gateway (SWG) mode, FortiSASE proxies traffic from the client. While being proxied, connections using secure protocols like HTTPS have their certificates replaced and signed by FortiSASE. To avoid seeing warnings and errors, the client must trust the signing certificate authority (CA) and have a valid certificate chain back to the root CA. Therefore, installing FortiSASE's CA certificate on the client's trusted certificate store is important.

You should provide users with the required CA certificate during onboarding. In SWG agentless mode, when you onboard users from the GUI, download the SWG certificates package that appears at the end of the *Secure Web Gateway Users* instructions. You can also find this on the right side of the *System* > *SWG Configuration* page.



For instructions demonstrate how to install certificates on various operating systems, see Installing a certificate for deep inspection mode on page 148.

Proxy configuration

To connect to FortiSASE in secure web gateway (SWG) mode, each endpoint client must configure proxy settings within its network or browser settings to point to FortiSASE's servers. You can configure this individually on the endpoint or, if you are using an enterprise management system, push it out to managed endpoints centrally.

You should provide users one of the following during the user onboarding process:

- URL to the hosted proxy autoconfiguration (PAC) file
- Proxy server addresses and port if users are to configure proxy settings manually.

From the *System* > *SWG Configuration* page, make note of the following information:

Field	Description
Global (Recommended)	Global FortiSASE server address for your instance.
Secure Web Gateway Server(s)	Lists address of each individual regional FortiSASE server for your instance.
Secure Web Gateway Port	Port that client should connect to in their proxy settings.
PAC File	Static copy of the PAC file, which you can customize and rehost on your server.
Hosted PAC File	Address of the PAC file hosted on the FortiSASE server.

See SWG Configuration on page 270.

Users are expected to have installed the FortiSASE certificate authority certificate on their devices. See Certificate installation on page 291.

Proxy settings on endpoint clients can differ between operating systems (OS) and browsers. While the following examples demonstrate the configuration for the selected OSes, refer to your OS or browser for complete instructions on configuring proxy settings.

- Windows on page 292
- macOS on page 293
- Chrome OS on page 294
- Managed Chromebook on page 295

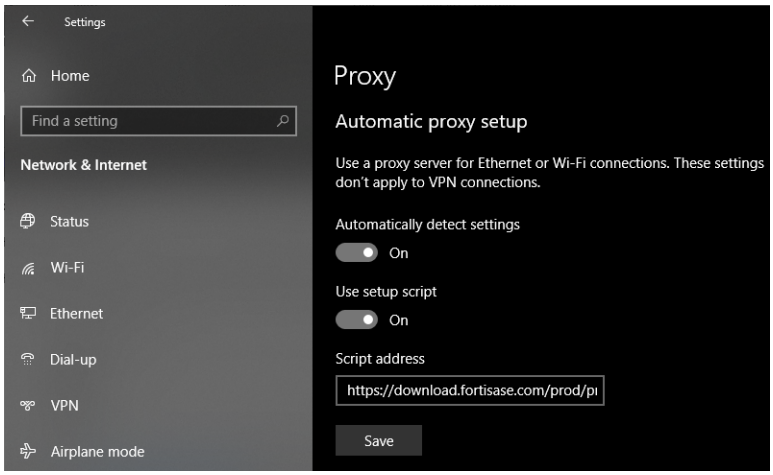
Windows

The end user can configure proxy settings at the operating system (OS) level or in a browser. When you configure Secure Web Gateway (SWG) settings at the OS level, Windows applies them to all installed browsers. The following gives instructions for configuring SWG settings at the OS level on a Windows 10 device.

To configure Windows 10 to use the FortiSASE SWG server:

1. In Windows, go to *Windows Settings* > *System* > *Proxy Settings*.
2. Enable *Use setup script*.

3. In the *Script address* field, enter the *Hosted PAC File* URL.



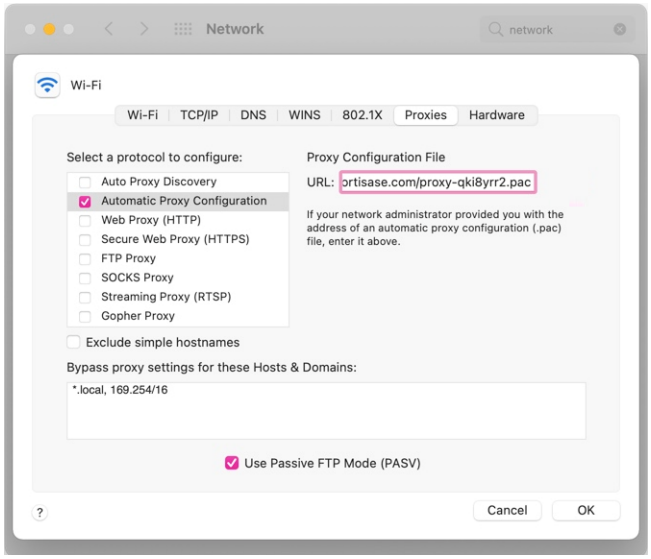
4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

macOS

This example demonstrates manually configuring proxy settings on macOS. See also Change proxy settings in Network preferences on Mac.

To manually configure proxy settings on a macOS endpoint:

1. Go to the *Apple menu* > *System Preferences* > *Network*.
2. In the list, select the Network service. For example, you may select your connected wireless SSID.
3. Click *Advanced*.
4. On the *Proxies* tab, select the protocol to configure. Enable *Automatic Proxy Configuration*, then enter the URL to your hosted PAC file.
5. Click *OK*, then apply to apply the changes.

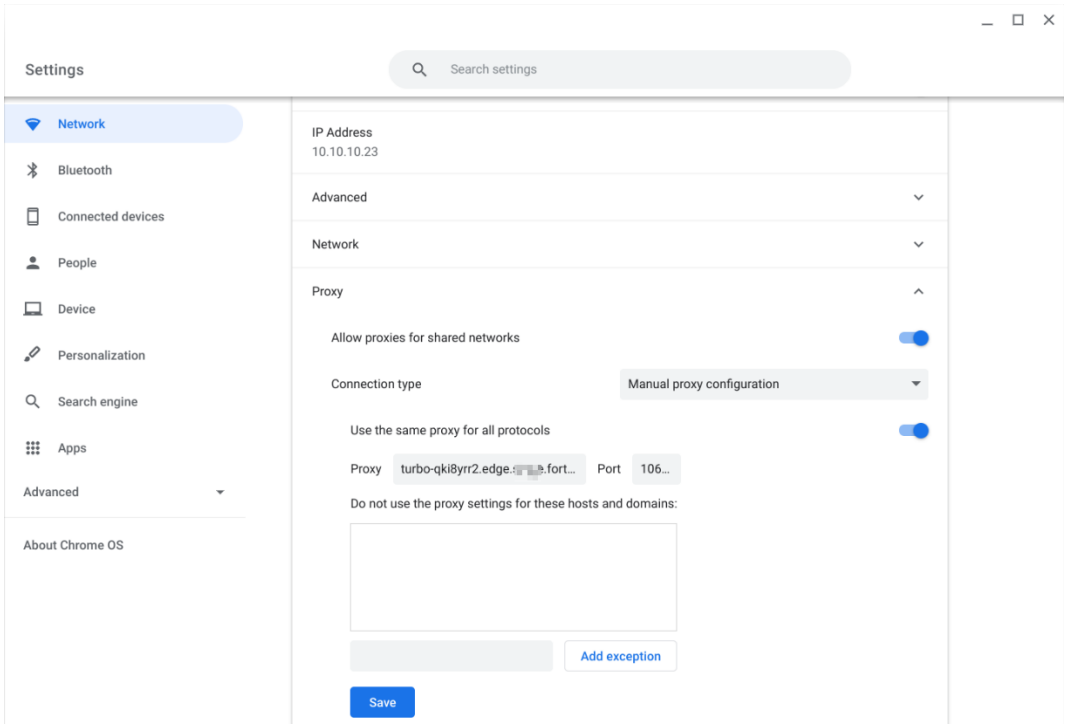


6. The next time that the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt to authenticate.

Chrome OS

To configure proxy as a system-wide setting:

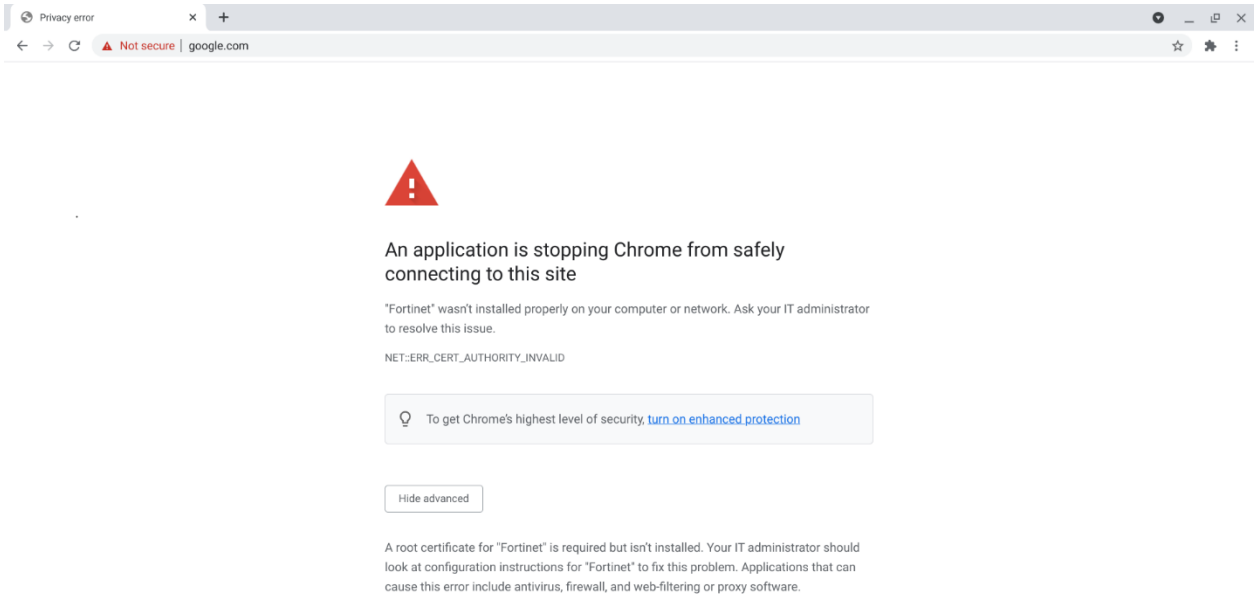
1. Open the Launcher, and search for *Settings*.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings.
4. For *Connection type*, select one of the following:
   a. Select *Automatic proxy configuration*. This is the recommended method. Point the *Autoconfiguration URL* to the FortiSASE-hosted PAC file.
   b. To configure manual proxy configuration, do the following:
      i. Select *Manual proxy configuration*.
      ii. Enable *Use the same proxy for all protocols*.
      iii. Enter the proxy server address, and the Secure Web Gateway port that your administrator provided. You can select the global proxy or the server closest to you.
      iv. Click *Save*.



If issues arise with some websites using SOCKS, you can work around this by disabling *Use the same proxy for all protocols*. Then only define the proxy server address for HTTP proxy and secure HTTP proxy.

5. On a successful connection, your browser prompts you to authenticate. Enter your user credentials to authenticate to FortiSASFortiSASE and continue browsing the web.

If you receive a warning message from Chrome preventing you to go further, you must disable your proxy settings, and install the FortiSASE certificate authority certificate before reenabling proxy.



Managed Chromebook

If your organization manages Chromebooks using the Google Admin console, you can centrally configure proxy settings on the Admin console and distribute them to each managed Chromebook.

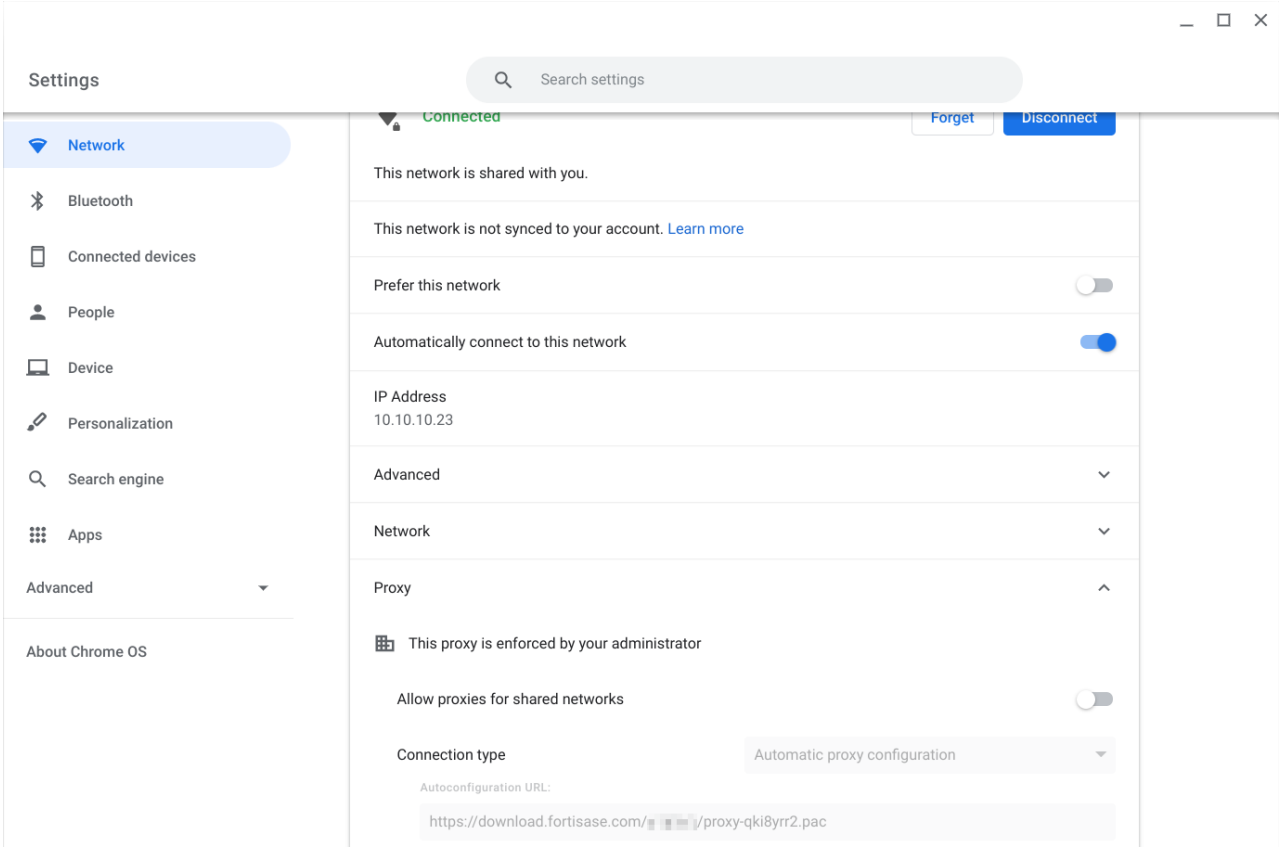
To configure proxy as a system-wide setting on Google Admin Console:

1. On the Google Admin console, go to *Device* > *Chrome* > *Settings* > *Users & Browsers.*.
2. Select the organizational unit in which to apply these settings.
3. Under *User and Browser Settings*, filter for the keyword `Proxy`. The *Network* section appears.
4. For *Proxy mode*, use one of the following options:
   a. Select *Always use the proxy auto-config specified below*. Enter FortiSASE's hosted PAC file address. Save.
   b. Select *Always use the proxy specified below*. Enter the proxy server URL in the format <proxy server address>:<SWG port>. Save.

To verify proxy settings are configured on the managed Chromebook:

1. Open the Launcher and search for Settings.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings. The settings pushed from the Google Admin Console appear

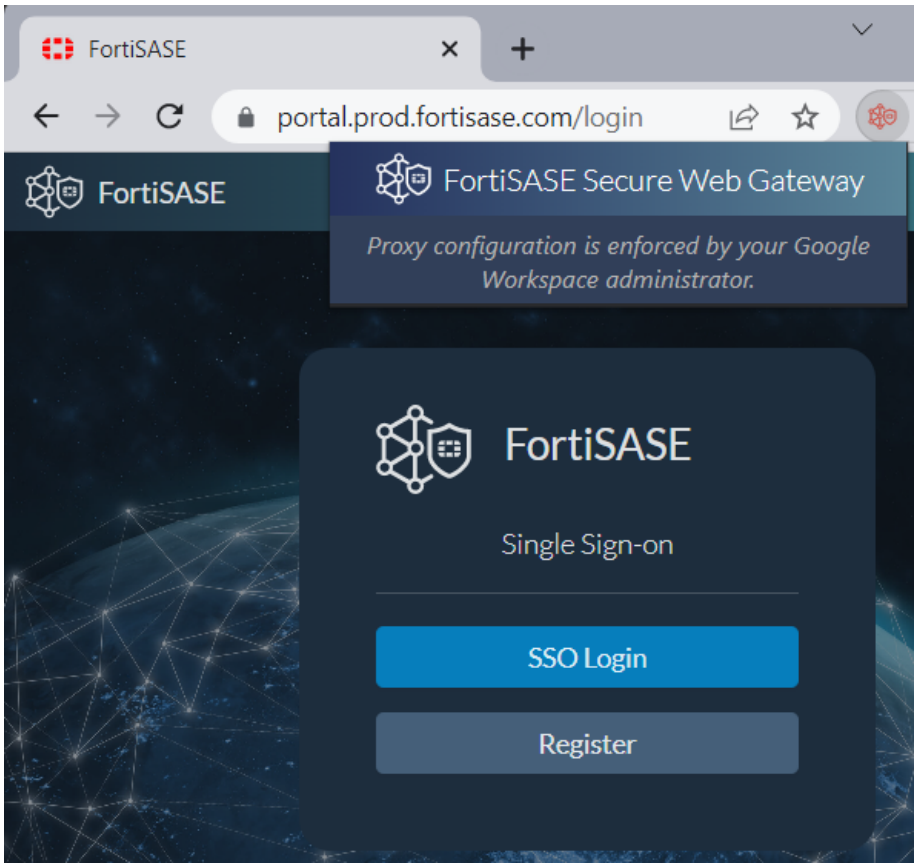
with an icon and warning that your administrator is enforcing this setting.



SWG Chrome extension and Chromebook support

FortiSASE supports a Chrome extension that allows enforcing FortiSASE secure web gateway (SWG) connectivity for selected endpoints with the Chrome browser installed, including Chromebooks, based on the endpoint operating system (OS) and the corresponding extension policy that the Google Workspace administrator configured.

You can download the FortiSASE Secure Web Gateway Chrome extension from the Google Chrome Web store and add it to the Chrome web browser.



This extension relies on the following features being configured in FortiSASE:

- SWG single sign-on
- SWG configuration

The extension also requires that the user has already downloaded and installed the SWG certificates to the device certificate store as Certificate installation on page 291 describes. Alternatively, you can use Google Workspace to install certificates on Chromebooks as Add and assign digital certificates for managed devices describes.

Since this extension is not installed in Chrome incognito mode, the administrator should disable incognito mode in Google Workspace.

This extension allows you to configure the following settings on an endpoint through Google workspace:

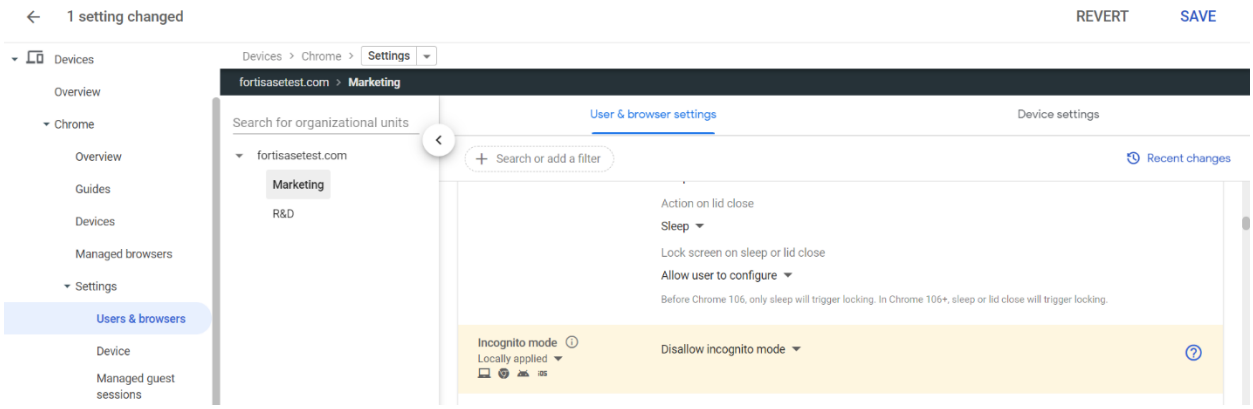
- Default or custom hosted PAC file URL
- User ability to view PAC file URL within the extension
- Configuration of supported platforms (ChromeOS, Linux, macOS, and Windows) where SWG is enforced

To disable incognito mode in Google Workspace:

Since this extension is not installed in incognito mode, SWG policies are not enforced when using incognito mode. The Google Workspace administrator must disallow incognito mode to ensure that SWG is always enforced on the Chromebook and other devices with managed Chrome browsers.

1. Go to *Devices* > *Chrome* > *Settings* > *Users & browsers*.
2. Select the desired organizational unit (OU).
3. Scroll to *Security* > *Incognito mode*.

4. From the dropdown menu, select *Disallow incognito mode*.
5. Click *Save*.



To configure the extension policy for FortiSASE SWG Chrome extension:

You can apply the FortiSASE SWG extension to one or more user OUs within Google Workspace. All users assigned within an OU that the FortiSASE SWG extension is applied to have the extension installed and SWG enforced on their Chromebook and Chrome browser.

1. In the Google Admin console, go to *Devices* > *Chrome* > *Apps & extensions* > *Users & browsers*.
2. Select the desired OU to install and enforce the FortiSASE SWG extension.
3. Add the Chrome extension to the OU by clicking the + button on the bottom right, clicking *Chrome app or extension by ID*, and searching using the ID aecejhdejcnfihadbfidmndehobfdpcc.
4. Select the *FortiSASE Secure Web Gateway extension* to push to Chromebooks and devices with managed Chrome browsers.
5. Configure the policy using the following parameters:

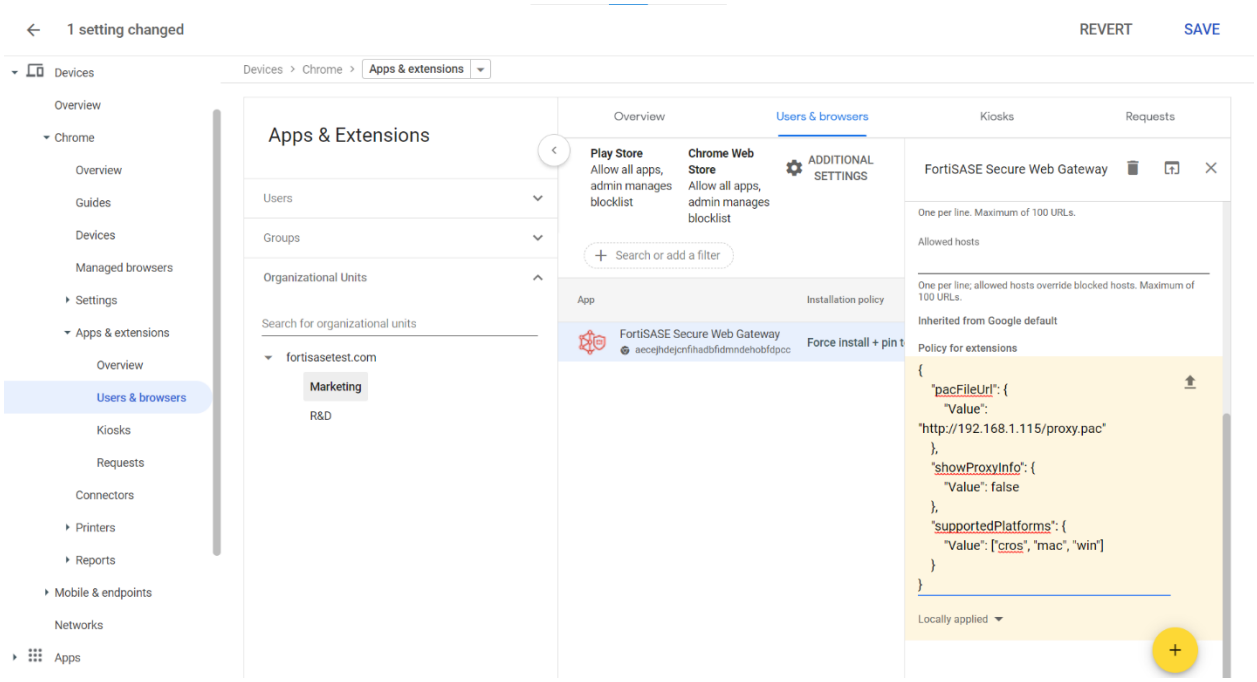
Parameter	Description
`pacFileUrl`	PAC file that the extension will enforce. Configure one of the following: • Default hosted PAC file link from FortiSASE in *System* > *SWG Configuration*. See SWG Configuration on page 270. • Custom hosted PAC file link from a server accessible to endpoints. See PAC file customization on page 286.
`showProxyInfo`	Possible values: `false` or `true`. • Setting this to `false` hides the PAC file URL from the extension. • Setting this value to `true` makes the PAC file URL visible to the extension.
`supportedPlatforms`	Possible values include `cros`, `linux`, `mac`, and `win` to specify ChromeOS (Chromebook), Linux, macOS, and Windows, respectively. To exempt a device from SWG enforcement, you can set one of these options: • Remove the device OS from the `supportedPlatforms` array • Set `pacFileUrl` to an empty string • Remove the `pacFileUrl` key-value pair from the policy configuration

6. Click *Save*.

Following is an example extension policy configuration using a custom PAC file hosted on a LAN server with the PAC file URL hidden from extension and the extension applied to ChromeOS, macOS, and Windows devices:

```
{
    "pacFileUrl": {
        "Value": "https://192.168.1.115/proxy.pac"
    },
    "showProxyInfo": {
        "Value": false
    },
    "supportedPlatforms": {
       "Value": ["cros", "mac", "win"]
    }
}
```

The following shows the FortiSASE SWG extension and example extension policy applied to users within the Marketing OU:



To verify the policy has been enforced on the device with the extension installed:

On the Chromebook or device with Chrome browser installed, go to chrome://policy from the Chrome browser to verify the aforementioned example policy has been enforced on the Chromebook or device with managed Chrome browser:

FortiSASE Secure Web Gateway

Policy name	Policy value	Source	Applies to	Level	Status	
pacFileUrl	https://192.168.1.115/proxy.pac	Cloud	Machine	Mandatory	OK, Superseding	Show more
showProxyInfo	false	Cloud	Machine	Mandatory	OK, Superseding	Show more
supportedPlatforms	["cros","mac","win"]	Cloud	Machine	Mandatory	OK, Superseding	Show more

Enterprise mobility management

FortiClient on different platforms supports integration with enterprise mobility management or mobile device management software. You can use this software to onboard endpoints to successfully connect to and be managed by FortiSASE.

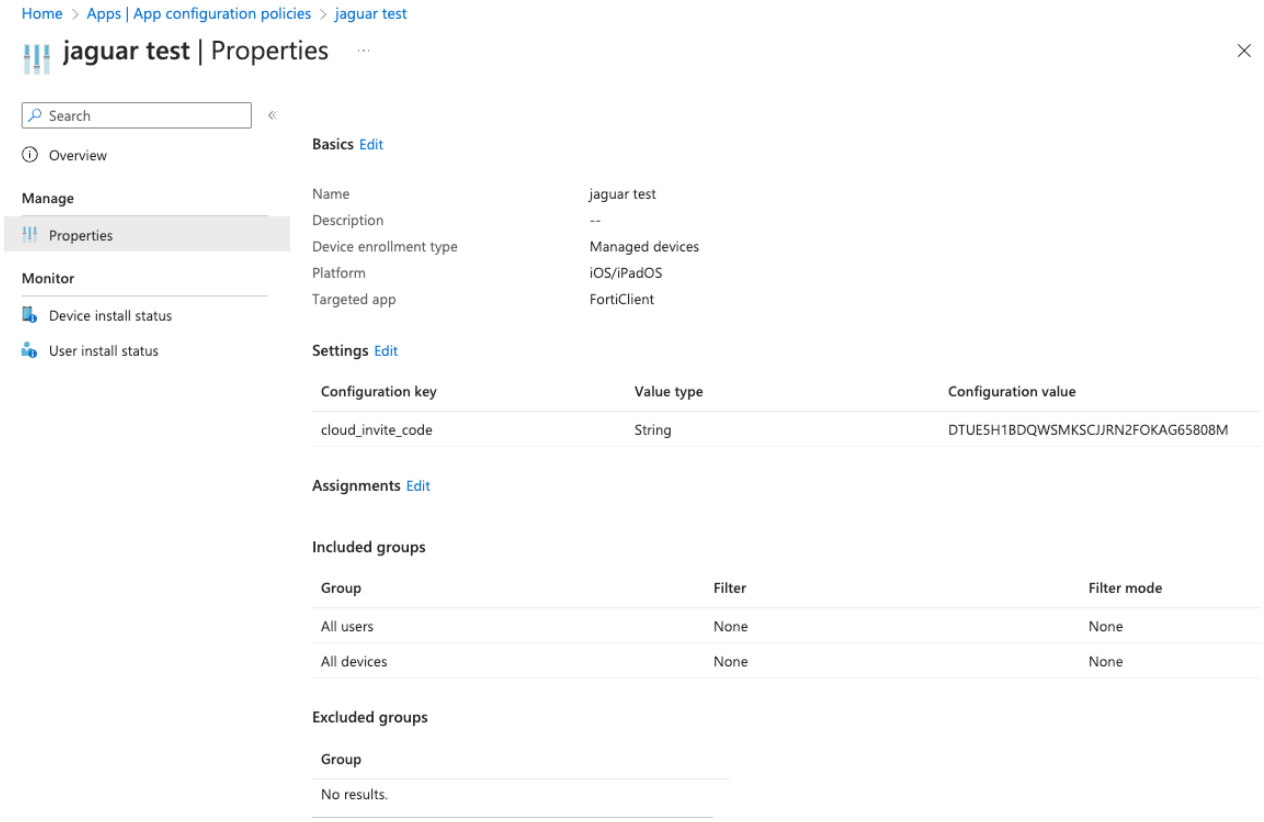
Configuring Microsoft Intune integration with FortiClient (iOS)

You can find details for configuring Microsoft Intune integration with FortiClient iOS in Configuring Microsoft Intune integration.

Configuring the FortiSASE invitation code

Since FortiSASE uses an invitation code instead of a direct IP address or hostname and port, ensure that `cloud_invite_code` is configured in one of the following locations in Intune:

- In the *Create app configuration policy* window on the *Settings* tab
- For an existing configuration policy, click *Properties* and check under *Settings*. In the example, you can see that `cloud_invite_code` is configured.



Deploying trusted certificates

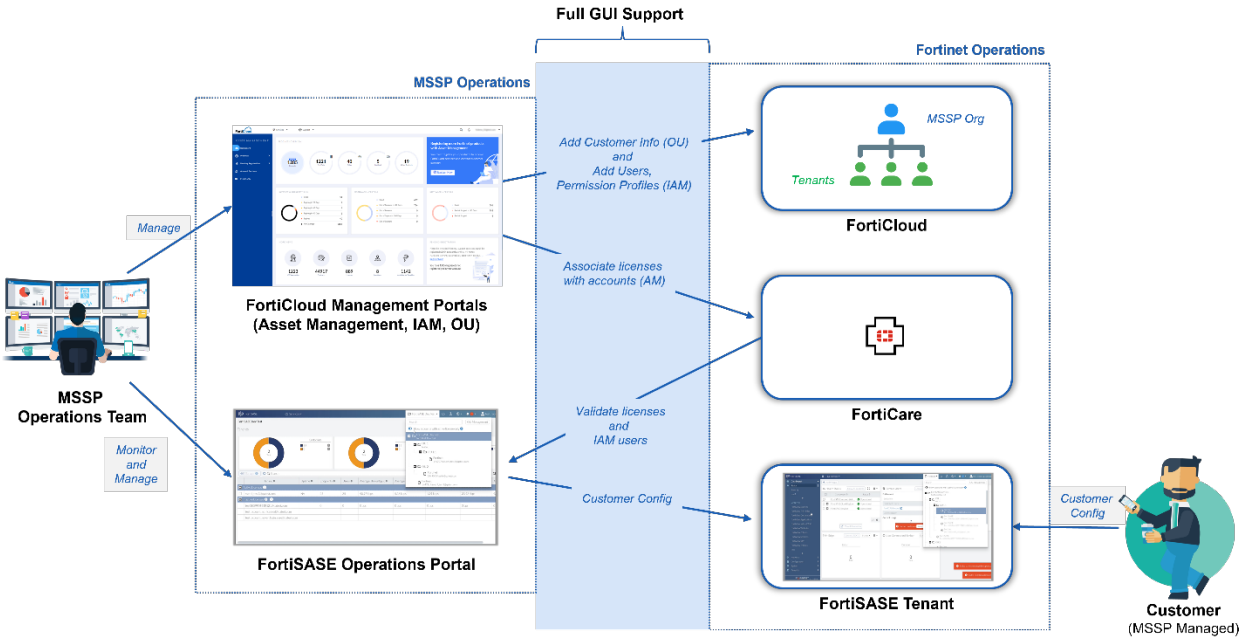
When FortiSASFortiSASE security components are configured to use SSL deep inspection, then the certificate authority (CA) certificate is automatically installed on desktop FortiClient endpoints. However, for mobile endpoints such as Apple devices running FortiClient iOS, then enterprise mobility management software must be used to install such CA certificates.

You can find details on deploying a trusted root certificate such as the CA certificate configured on FortiSASE for SSL deep inspection in Trusted root certificate profiles for Microsoft Intune.

MSSP portal

FortiSASE includes a portal that managed security service providers (MSSP) can use to offer their end customers a managed FortiSASE service by performing the following management functions for multitenant FortiSASE deployments:

- Monitor tenants' FortiSASE instances
- Access and manage tenants' FortiSASE instances



The FortiSASE MSSP portal is based on the use of FortiCloud Identity & Access Management (IAM) users and the FortiCloud organizational unit structure. For details, see Organization Portal and Identity & Access Management (IAM), respectively.

Prerequisites

You must apply a FortiCloud Premium contract to the root account to allow it to establish an organization and invite other FortiCare accounts to join the organization.

Configuration workflow

The workflow for configuring FortiCloud Identity Access & Management (IAM) users and organization units (OU) and using the managed security service provider (MSSP) portal is as follows:

1. Using the FortiCloud Organization portal:
   a. Enable organizations. See Enabling Organizations.
   b. Create an organization. See Creating an organization.
   c. Add one or more OUs. See Adding and deleting OUs.
   d. Add accounts to OUs by doing one of the following:
      - Invite FortiCloud accounts to join OUs. See Invitations and Creating invitation tokens. Then approve invitations to FortiCloud accounts. See Invitation Approval for details.
      - Create new member accounts linked to a real email address or a new placeholder email address generated at the same time as the member account. See Creating new Member Accounts.
2. Using the FortiCloud IAM portal:
   a. Set up a resource-based permission profile allowing IAM users to access FortiSASE as a portal. See Resource-based permissions on page 304.
   b. Configure IAM users. See Creating users, user groups, and roles within Organizations and Adding IAM users.
3. From the FortiSASE portal:
   a. When an IAM user logs in to FortiSASE for the first time, there are some preliminary steps to complete to validate the new IAM user. See Validating new IAM users.
   b. Access the MSSP portal using an IAM user corresponding to the root account. See Accessing the MSSP portal on page 312.
   c. Monitor tenants' FortiSASE instances. See Monitoring a tenant's instance on page 313.
   d. Manage tenants' FortiSASE instances. See Managing a tenant's instance on page 314.

For initially provisioning a tenant's FortiSASE instance, you can use one of the following approaches:
- By directly logging in to the FortiSASE portal, the customer's tenant administrator can provision the instance themselves.
- From the MSSP portal, the MSSP operations team with administrator access to the tenant can provision the instance and preconfigure it on behalf of the tenant.

For details on configuring FortiCloud OUs and adding FortiCloud accounts to OUs, see Organization Portal.

For details on creating new member accounts and managing them, see Creating new Member Accounts and Managing Member Accounts.

For details on configuring FortiCloud IAM users and permission profiles, see Identity & Access Management (IAM).

When configuring IAM users for an organization, you typically configure the user type as *Organization* with a *Permission Scope* configured to an organization unit (OU) or sub-OU. These users can access the MSSP portal.

IAM users where the user type is configured as *Local* can directly access the FortiSASE portal into a specific tenant's instance. However, they cannot access the MSSP portal.

When an IAM user with access to only a single account logs in to the FortiSASE portal, the FortiSASE portal for the instance loads instead of the MSSP portal.

When new member accounts with new placeholder email addresses, also known as placeholder accounts, have been added to sub-OUs, administrators of these sub-OUs can provision new instances associated with these placeholder accounts from the MSSP portal

Resource-based permissions

Permission control is global to the FortiSASE portal and provides the following privileges for each resource:

- No access
- Read/Write access
- Read-only access

If an IAM user is assigned a permissions profile with No access configured for all FortiSASE portal resources, then the IAM user will not be able to log into the FortiSASE portal.

The FortiSASE portal has the following resource categories:

Resource	Provide control over...
User & Authentication on page 305	User and authentication related settings.
Policy on page 305	VPN, SWG, and SPA policies.
Logging on page 307	Logging and reports features.
Monitoring on page 307	Monitoring features including FortiView, Digital Experience Monitoring, Managed Endpoints, and other monitor widgets.
Dashboards on page 308	Dashboard features.
Network on page 309	Network features including edge devices, SPA, DNS, hosts, services, and feeds.
System on page 310	System settings.
Security on page 310	Security profile groups and security features.
Endpoint Management on page 311	Managed Endpoints page, endpoint profiles, and ZTNA settings.
Infrastructure on page 311	FortiSASE provisioning.

See Permission profiles within Organizations.

Access to specific pages and actions require permissions to multiple resources.

In the table below, for entries marked with *Read-only access* involving allow or show actions, this privilege indicates the minimum privilege level required, which means the higher privilege level of *Read/Write access* can also be used in these cases.

On the other hand, for entries marked with *Read-only access* involving blocking or hiding actions, this privilege is the only privilege needed to achieve the desired actions.

User & Authentication

Action	User & Authentication	Monitoring	Endpoint Management	System
Allow viewing of *Connected Users* page, and *Remote Users* and *User Connection Monitor* widgets	Read-only access			
Onboard users button redirects to *Client Onboarding* documentation	Read-only access			
Block import/export of users and groups	Read-only access			
Allow viewing of users, PKI users, and groups	Read-only access			
Allow viewing of LDAP/RADIUS servers and users	Read-only access			
Hide *VPN user SSO* page	Read-only access			
Allow editing of *VPN User SSO* page	Read/Write access		Read/Write access	
Make *Show in FortiView* unavailable in *User Connection Monitor*	Read/Write access	No access		
Make *View Endpoint Details* unavailable in *Managed Endpoints* widget/page	Read/Write access		No access	
Hide *SWG user SSO* page	Read/Write access			No access

Policy

Action	Policy	User & Authentication	Network	Logging	Monitoring	Security	Endpoint Management
Allow users and groups to be viewed from policies	Read/Write access	Read-only access					
Allow users and groups to	Read/Write access	Read/Write access					

Action	Policy	User & Authentication	Network	Logging	Monitoring	Security	Endpoint Management
be created inline from policies							
Allow creating hosts, feeds, and services inline within policies	Read/Write access		Read/Write access				
Hide private access policies	Read/Write access		No access				
Allow creating ZTNA tags in-line within policies	Read/Write access						Read/Write access
Allow *Show Matching Traffic Logs* when a policy is right-clicked	Read/Write access			Read-only access			
Allow *Show in FortiView* when a policy is right-clicked	Read/Write access				Read-only access		
Allow creating security	Read/Write access					Read-only access	

Action	Policy	User & Authentication	Network	Logging	Monitoring	Security	Endpoint Management
profile groups inline within policies							

Logging

Action	Logging	Network
Allow downloading of generated reports	Read-only access	
Allow scheduled reports to be viewed	Read-only access	
Allow *Analytics* > *Settings* page to be viewed	Read-only access	
Hide private access tab from *Traffic* logs	Read/Write access	No access

Monitoring

Action	Monitoring	User & Authentication	Dashboards	Network	Endpoint Management
Hide *FortiView* monitors, *Digital Experience Monitoring (DEM)*, *Managed Endpoints*, *User Connection Monitor*, *Application Bandwidth*, and *Bandwidth Monitor* widgets	No access				
Show *Asset Map*, *DEM*, *Managed Endpoints*, and *Connected Users* pages	Read-only access				
Hide *Subscribe* button from *Health* widget	Read-only access				
Allow downloading FortiClient logs from	Read/Write access				Read-only access

Action	Monitoring	User & Authentication	Dashboards	Network	Endpoint Management
Endpoint details slide-in					
Allow requesting FortiClient logs from *Endpoint* details slide-in	Read/Write access				Read/Write access
Allow DEM endpoint features from *Endpoint* details slide-in	Read/Write access				Read/Write access
Block ability to modify *Management Connection* status of endpoints	Read/Write access				No access
Allow add, edit, delete of FortiView monitors in *Dashboards*	Read/Write access		Read/Write access		
Hide SPA hubs and edge devices from *Asset Map*	Read/Write access			No access	
Hide *Connected Users* link from *Asset Map*	Read/Write access	No access			
Hide *Deauthenticate* button from *Connected Users* page and *User Connection Monitor* widget	Read/Write access	Read-only access			

Dashboards

Action	Dashboards	User & Authentication	Monitoring	Network	Security	Endpoint Management
Block ability to create, edit, delete, and resize widgets	Read-only access					
Block ability to add FortiView and monitor widgets	Read/Write access		No access			
Block ability to add widgets related to	Read/Write access			No access		

Action	Dashboards	User & Authentication	Monitoring	Network	Security	Endpoint Management
private access and edge devices						
Block ability to add *Managed Endpoints* and *Vulnerability Summary* widgets	Read/Write access					No access
Block ability to add *User Connection Monitor* and *Remote Users* widgets	Read/Write access	No access				
Block ability to add *Internet Access Security Status* widget	Read/Write access				No access	

Network

Action	Network
Show *Edge Devices (FortiAPs, FortiExtenders, FortiGates)*, *Secure Private Access*, *DNS*, *Hosts*, *Services* and *Feeds* pages	Read-only access
Hide *Update authentication method*, *Service Connection Priorities*, *Edit* and *Delete* buttons from *Network* > *Secure Private Access* > *Service Connections* tab	Read-only access
Hide *Create*, *Edit*, and *Delete* buttons for *Hosts*, *Services*, *Feeds*, and *DNS* pages	Read-only access
Disable *Authorize*, *Deauthorize*, and *Disconnect* actions for Edge	Read-only access

Action	Network
Devices	
Hide notifications for newly discovered edge devices	Read-only access

System

Action	Network
Block import, download, and delete actions for certificates	Read-only access
Block save and edit of HTML templates	Read-only access
Block create, edit, and delete of images in *HTML templates* > *Images* tab	Read-only access
Hide *System* section	No access

Security

Action	Security	Logging	Monitoring	Network
Block ability to create, edit, or delete security profile groups	Read-only access			
Block ability to enable or disable security features	Read-only access			
Block ability to create, edit, or delete profile resources	Read-only access			
Hide *View Logs* buttons from all security features	Read/Write access	No access		
Hide *View All* buttons from all security features	Read/Write access		No access	
Display threat data in the security features cards	Read/Write access	Read-only access	Read-only access	
Hide the *Private Access* tab in the *Configuration* > *Security* > *Profiles* page	Read/Write access			No access
Show the *Private Access* tab and allow renaming, deleting, and customizing of private access security profile groups	Read/Write access			Read-only access

Endpoint Management

Action	Endpoint Management	Monitoring
Allow downloading FortiClient logs from *Endpoint* details slide-in	Read-only access	Read/Write access
Allow requesting FortiClient logs from *Endpoint* details slide-in	Read/Write access	Read/Write access
Allow DEM endpoint features from *Endpoint* details slide-in	Read/Write access	Read/Write access
Block ability to modify *Management Connection* status of endpoints	Read-only access	
Hide *More Options* > *Show in FortiView* in *Managed Endpoints* page	Read/Write access	No access

Infrastructure

Action	Infrastructure
Block provisioning of FortiSASE instance	Read-only access or No access

Using the MSSP portal

After configuring the required settings in the FortiCloud Identity & Access Management (IAM) portal and FortiCloud Organization portal, you can access the managed security service provider (MSSP) portal.

The MSSP portal allows MSSP administrators to provide a managed FortiSASE service to end customers by performing these tasks:

1. When an IAM user logs in to FortiSASE for the first time, there are some preliminary steps to complete to validate the new IAM user. See Validating new IAM users.
2. Access the MSSP portal using an IAM user corresponding to the root account. See Accessing the MSSP portal on page 312.
3. Monitor the status of a tenant's FortiSASE instance. See Monitoring a tenant's instance on page 313.
4. Manage a tenant's FortiSASE instance, namely, to preconfigure it prior to delivery to the end customer, troubleshoot it, and resolve any configuration issues that the end customer reports. See Managing a tenant's instance on page 314.

Accessing the MSSP portal

The managed security service provider (MSSP) portal requires configuring an Identity & Access Management (IAM) user corresponding to the root account, as Adding IAM users describes.

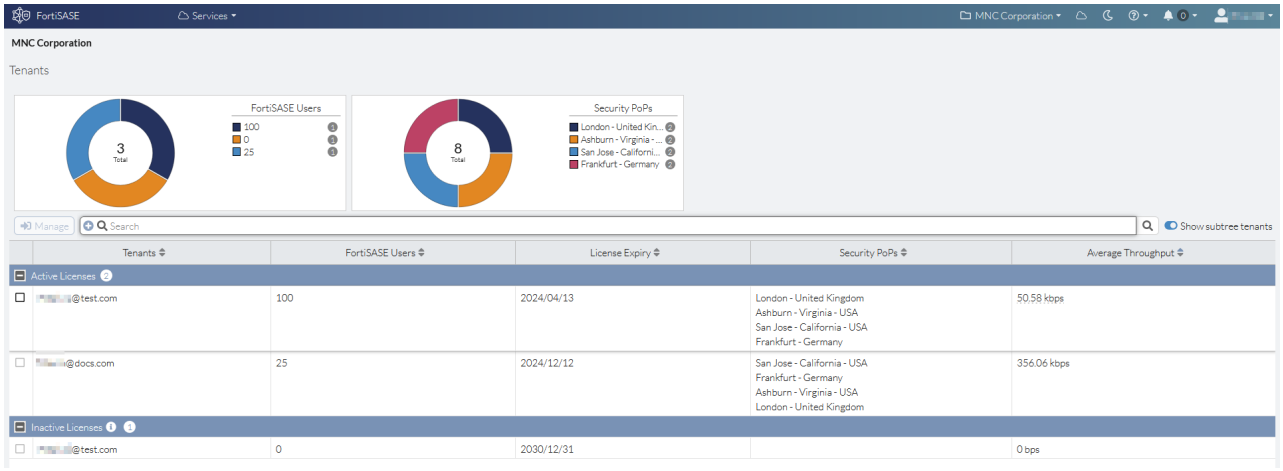
When configuring IAM users for an organization, you typically configure the user type as *Organization* with a *Permission Scope* configured to an organization unit (OU) or sub-OU. These users can access the MSSP portal.

IAM users where the user type is configured as *Local* can directly access the FortiSASE portal into a specific tenant's instance. However, they cannot access the MSSP portal.

When an IAM user with access to only a single account logs in to the FortiSASE portal, the FortiSASE portal for the instance loads instead of the MSSP portal.

To access the MSSP portal from the FortiSASE portal:

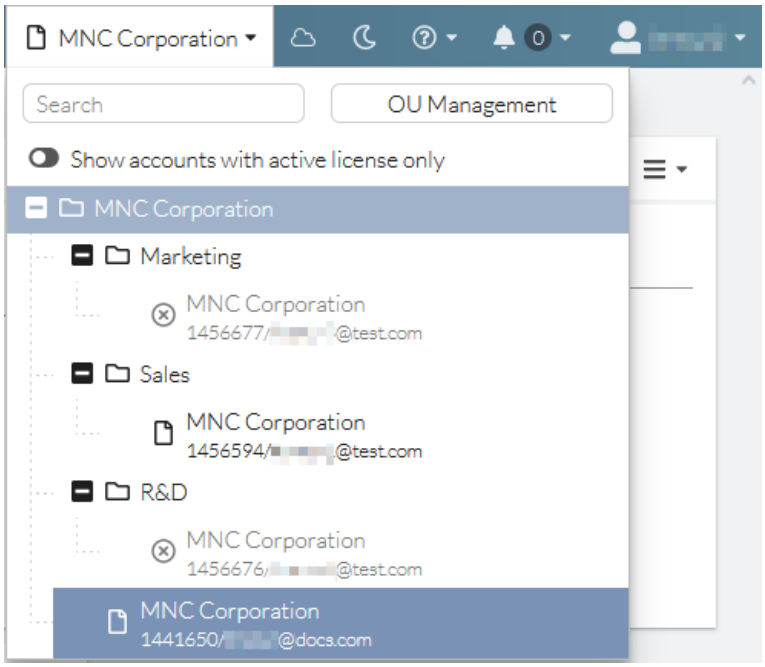
1. Go to the FortiSASE portal.
2. Click *SSO Login*.
3. Click *Sign in as IAM user*.
4. Log in with the user credentials from the CSV that you downloaded when creating the IAM user in To create an IAM user with the wizard. The MSSP portal for the organization displays.



To access the MSSP portal from within a FortiSASE instance:

1. From within a FortiSASE instance, select the context switch dropdown menu. Accounts within the organization display.
2. Select the organization or sub-organization units (OU) to enter the MSSP portal for the selected context. In the example, selecting the top-level organization MNC Corporation displays FortiSASE instances for all OUs. Selecting

the Sales OU displays FortiSASE instances for that OU only.



Monitoring a tenant's instance

Once logged into the managed security service provider portal, the administrator CAN monitor the following FortiSASE tenant data:

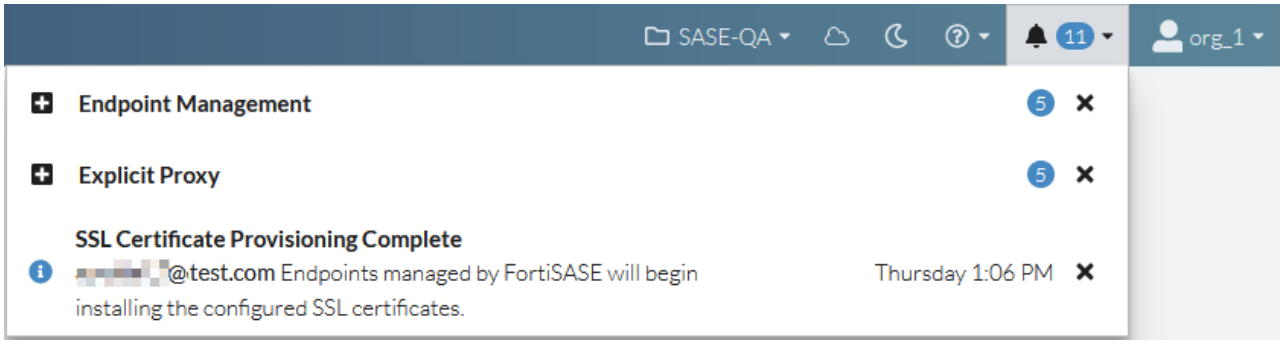
- Pie charts showing the distribution of FortiSASE users for active and inactive licenses and the distribution of security points of presence (PoP)
- Tenant entries separated into *Active Licenses* and *Inactive Licenses* categories. The *Inactive Licenses* category is for tenants for which data is not yet available for instances that are not yet provisioned.
- When *Show subtree tenants* is enabled, tenants for second- and third-level organization units (OU) display. When this toggle is disabled, only tenants for the first-level OU (top-level organization only) display.
- Columns with data display. The following lists all available columns. Bolded columns display by default:

Column	Description
Tenants	FortiSASE tenant listed with its Identity & Access Management user email address.
FortiSASE Users	Number of licensed users associated with the tenant.
License Expiry	FortiSASE user license expiry date.
Security PoPs	List of security PoPs associated with a tenant.
Average Throughput*	Average transmitted data rate through the tenant's instance.
Average Egress In*	Average received data rate for tenant's egress interface.
Average Egress Out*	Average transmitted data rate for tenant's egress interface.

Column	Description
Average Ingress In*	Average received data rate for tenant's ingress interface.
Average Ingress Out*	Average transmitted data rate for tenant's ingress interface.

* Bandwidth shown is an average for the last 24 hours.

- The bell icon in the banner displays notifications for all tenants within the selected OU. If you select a sub-OU, the MSSP portal filters notifications for that sub-OU.



Managing a tenant's instance

A managed security service provider (MSSP) administrator can use the MSSP portal to select a tenant and manage its FortiSASE instance. This allows the MSSP administrator to preconfigure the instance prior to handing off the instance to end customer and to troubleshoot and resolve any configuration issues if the end customer reports any issues with the instance.

For initially provisioning a tenant's FortiSASE instance, you can use one of the following approaches:

- By directly logging in to the FortiSASE portal, the customer's tenant administrator can provision the instance themselves.
- From the MSSP portal, the MSSP operations team with administrator access to the tenant can provision the instance and preconfigure it on behalf of the tenant.

When an IAM user with access to only a single account logs in to the FortiSASE portal, the FortiSASE portal for the instance loads instead of the MSSP portal.

To manage a tenant's FortiSASE instance from the MSSP portal using the Manage button:

1. From the MSSP portal, in the *Active License* category, click a tenant.
2. Click *Manage*.
3. The tenant's FortiSASE instance loads as if you logged into the FortiSASE portal using the Identity & Access Management (IAM) user account associated with the instance.
4. Perform any configuration within the FortiSASE instance with the same permissions as the IAM user account associated with the instance.

To manage a tenant's FortiSASE instance from the MSSP portal using the context switch dropdown menu:

1. From within a FortiSASE instance, select the context switch dropdown menu. Accounts within the organization display.
2. Enable *Show accounts with active license only* to filter the dropdown menu to only display organization units and accounts with active licenses.
3. Select the IAM user or member account (with a real or placeholder email address) whose FortiSASE instance you want to manage.
4. The tenant's FortiSASE instance as if you had logged into the FortiSASE portal using the account associated with the instance.
5. Perform any configuration within the FortiSASE instance with the same permissions as the account associated with the instance.

When new member accounts with new placeholder email addresses, also known as placeholder accounts, have been added to sub-OUs, administrators of these sub-OUs can provision new instances associated with these placeholder accounts from the MSSP portal

SPA for an MSSP hub

For the MSSP hub use case, see SPA for an MSSP hub.

Troubleshooting

FortiSASE supports the FortiGate Support Tool. The FortiGate Support Tool is a Google Chrome extension that can execute background debugs on the FortiSASE GUI to troubleshoot errors. Using the tool, you can create a file to provide to the Fortinet Support for troubleshooting. See Troubleshooting Tip: GUI slowness and errors via FortiGate support tool.

FAQs

Dedicated public IP addresses

Implementing dedicated public IP addresses is currently impactful to the operation of the FortiSASE instance. FortiSASE Operations recommends that a request to implement dedicated public IP use cases be raised with ample time in advance before onboarding any remote users or implementing features such as FortiAP, FortiExtender, or FortiGate edge device support to avoid service disruption.

What is the expected impact of applying the FortiSASE-Dedicated-IP add-on license to an existing FortiSASE instance with a Standard license?

The following impact is expected for an existing FortiSASE instance:

- Approximately a 2 to 4-hour scheduled maintenance window is expected.
- During the maintenance window, users will periodically be disconnected and will need to manually reconnect.
- Intermittently, DNS will not resolve at all, and as a result, users will not be able to connect.
- Occasionally, DNS may resolve to the incorrect PoP due to health check application so users may be directed to the wrong regions and will need to manually reconnect once completed for best performance.
- Secure web gateway (SWG) and Thin Edge configuration settings may need to be disabled/reconfigured.

What is the expected impact of applying source IP anchoring to an existing FortiSASE instance once all proper licensing is in place?

For source IP anchoring, you must purchase another Dedicated Public IP add-on license with four additional dedicated IP addresses beyond the initial number of dedicated IP addresses per PoP. The additional four dedicated IP addresses can be allocated as desired for source IP anchoring rules such as all in a single PoP, one per PoP, or any combination in between.

Source IP Anchoring is an additional feature beyond dedicated IP provisioning and may require an extra 2-4 hours to implement on an existing FortiSASE instance, depending on the complexity of requirements.

Licensing

I am an existing customer with a registered legacy FortiSASE device-based license (EMS05-434) or a registered FortiSASE user-based license (EMS05-553). I want to purchase the FortiSASE standard user license (EMS05-547), Advanced user license (EMS05-676), or the Comprehensive user license (EMS-759). What should I do?

The device-based and user-based licenses cannot be combined or directly converted.

No FortiSASE reconfiguration is required. The process involves proper FortiSASE license management with the assistance of Fortinet Customer Service.

Therefore, as an existing customer, you must follow this process:

- If your license has a remaining term and has not yet expired:
  a. Contact your Fortinet Sales or Partner contact to provide you with assistance with converting the existing license to a FortiSASE user Standard, Advanced, or Comprehensive license. See the SASE and Zero Trust Ordering Guide.
  b. Contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal to review license conversion options available for your device-based license (EMS05-434) or for your user-based license (EMS05-553).
- If your license has expired:
  a. Contact your Fortinet Sales or Partner contact to purchase a new FortiSASE user Standard, Advanced, or Comprehensive license. See the SASE and Zero Trust Ordering Guide.
  b. Once you have purchased a new FortiSASE user license, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with removing the expired license from your account and applying the new one to your account. The FortiSASE serial number should be preserved.

I am an existing customer with the FortiSASE standard user license (EMS05-547) and want to upgrade to an Advanced user license (EMS05-676), or the Comprehensive user license (EMS-759). What should I do?

No FortiSASE reconfiguration is required. The license upgrade requires proper FortiSASE license management with the assistance of Fortinet Customer Service.

Therefore, an existing customer, you must follow this process:

1. Obtain a FortiSASE Advanced or Comprehensive user license:
   - If your license has a remaining term and has not yet expired, contact your Fortinet Sales or Partner contact to provide you with assistance with co-terming the existing license to a FortiSASE user Advanced, or Comprehensive license. This requires obtaining a co-term quote from the Fortinet Renewals team. See the SASE and Zero Trust Ordering Guide.
   - If your license has expired, contact your Fortinet Sales or Partner contact to purchase a new FortiSASE user Advanced, or Comprehensive license. See the SASE and Zero Trust Ordering Guide.
2. Once you have a converted FortiSASE license or have purchased a new FortiSASE user license, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with removing the older license from your account and applying the new one to their account. The FortiSASE serial number should be preserved.

I am an existing customer with the FortiSASE standard user license (EMS05-547), Advanced user license (EMS05-676), or Comprehensive user license (EMS-759). I want to shift to using FortiSASE user licenses in FortiFlex. What should I do?

Shifting from term-based licensing to FortiFlex licensing results in a new FortiSASE serial number being created. In other words, a new FortiSASE instance with default configuration is created.

The current FortiSASE configuration is lost after the licensing shift, and there is no option to restore the old configuration on the new FortiSASE instance. Therefore, FortiSASE reconfiguration is required. It is strongly recommended that you perform this licensing shift before fully deploying FortiSASE. Before proceeding with these steps, ensure you are familiar with the currently configured features and their settings and the use cases serviced by your current FortiSASE deployment and understand the consequences of this license shift.

This license shift requires proper FortiSASE license management with the assistance of Fortinet Customer Service.

Therefore, an existing customer, you must follow this process:

1. Contact your Fortinet Sales or Partner contact to purchase new FortiFlex Program and Point Pack SKUs for access to the FortiFlex portal from within your FortiCloud account. See the FortiFlex Program Ordering Guide.
2. After your existing license has expired, obtain a FortiSASE Standard, Advanced or Comprehensive user license using FortiFlex.
3. Once you have a converted FortiSASE user license or have generated a FortiSASE user license from FortiFlex, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with these steps:
   a. Removing the older license from your account and applying the new one to their account, which results in a new FortiSASE serial number being created.
   b. Creating a new Technical Support ticket to engage Fortinet technical teams to request the deletion the old instance on the backend (may take up to two business days).
4. At this point, a new FortiSASE serial number is created. In other words, a new FortiSASE instance with default configuration is created. The current FortiSASE configuration is lost after the licensing shift, and there is no option to restore the old configuration on the new FortiSASE instance. Therefore, FortiSASE reconfiguration is required. Configure your FortiSASE instance with desired features from your previous deployment.
5. Perform the configuration in FortiSASE by logging in with the root principal email.
   a. Review FortiSASE documentation for details on configuring features.
   b. Review FortiSASE 4-D deployment guides for details on configuring common use cases and deployments.
   c. For Advanced or Comprehensive licenses, make use of *Assisted Onboarding*. See *FortiSASE Support Services* in the SASE and Zero Trust Ordering Guide.
6. If you want Fortinet to perform the endpoint management configuration in FortiSASE, purchase Fortinet Professional Services, and request either the **Advanced Deployment Service** or **Custom service engagement**. See *FortiSASE Support Services* in the SASE and Zero Trust Ordering Guide.

PoPs

What is the expected impact of applying any region or security point of presence (PoP) changes to an existing FortiSASE instance once all proper licensing is in place?

The number of security PoPs that are accessible by remote users depends on the FortiSASE license tier and number of users. See Number of security data centers accessible per license on page 325.

The following impact is expected for an existing FortiSASE instance for any PoP changes, such as adding or deleting PoPs:

- Approximately a 2 to 4-hour scheduled maintenance window is expected.
- Occasionally, DNS may resolve to the incorrect PoP due to health check application so users may be directed to the wrong regions and will need to manually reconnect once completed for best performance.

Shifting from FortiClient EMS to FortiSASE

I am an existing customer with a FortiClient EMS on-premises deployment. What is the path to move my endpoints to FortiSASE?

FortiSASE includes its own instance of EMS as part of the service, and it is required for proper orchestration of the solution. Therefore, customers with an existing FortiClient EMS solution will need to shift to using the FortiSASE instance of EMS.

Currently, the shift from an existing FortiClient EMS on-premises deployment to FortiSASE does not preserve FortiClient Cloud configuration because it will be replaced with configuration defined for FortiSASE after the process is completed. You must configure endpoint features supported in FortiSASE. See How can I configure FortiSASE for endpoint management? on page 323

The process below should allow endpoints to be shifted from FortiClient Cloud to FortiSASE without the need for a third-party endpoint management system.

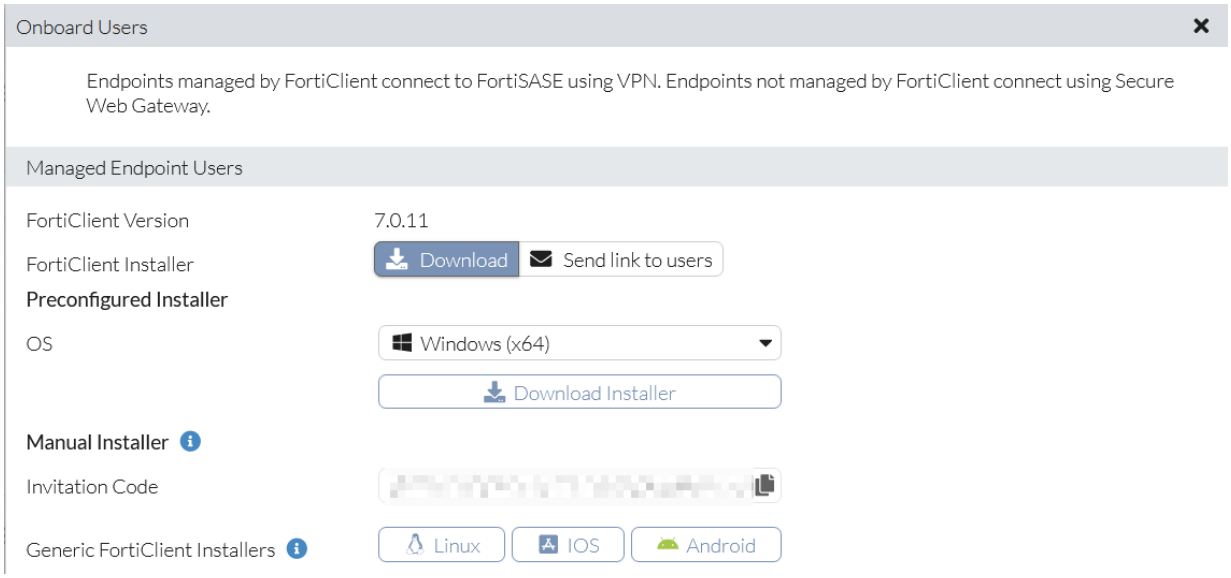
You must follow this process:

1. Contact your Fortinet Sales or Partner contact to perform one of these steps:
   - For an existing FortiClient subscription, a.k.a. the FortiClient FortiTrust license, to provide you with assistance with converting it to a FortiSASE user-based Standard, Advanced, or Comprehensive license
   - For an expired FortiClient subscription, to provide you assistance with purchasing a new FortiSASE user-based license.

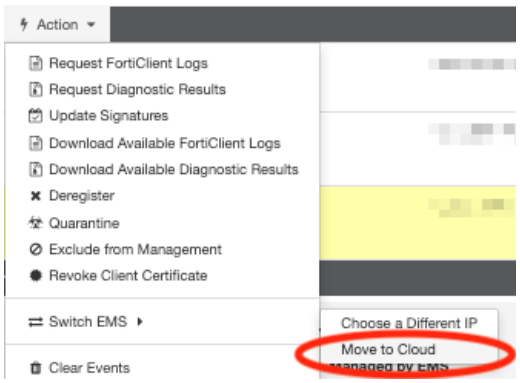
   See the SASE and Zero Trust Ordering Guide.
2. Once you have a FortiSASE user-based license, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with these steps:

a. Removing the FortiClient FortiTrust license from your FortiCloud root principal account (may take up to three business days).
b. Applying the new FortiSASE user-based license to your account.

3. Log into the FortiSASE portal and provision your instance according to the steps in the Cloud Deployment guide, if it has not been provisioned previously.
4. In the FortiSASE portal, obtain the invitation code as follows:
   a. Go to *Dashboards* > *Status*.
   b. Under the *Remote Users* widget, click *Onboard Users*. If this widget does not exist, click *+Add Widget* and add a new *Remote Users* widget.
   c. In *Onboard Users*, under *Managed Endpoint Users* and under *Manual Installer*, click the copy icon to the right of the *Invitation Code* text field to copy the invitation code to the clipboard.

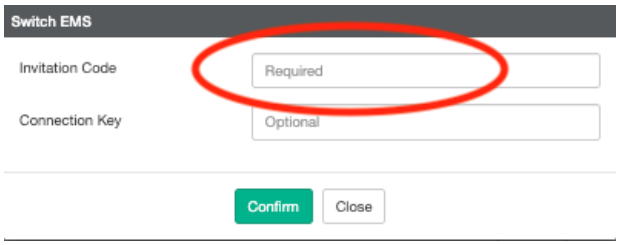


   d. Paste the invitation code to a text file for later use.
5. In the FortiClient EMS GUI, move the FortiClient endpoints as follows:
   a. Go to *Endpoints*.
   b. Select the desired endpoints to move.
   c. Select *Action* > *Switch EMS* > *Move to Cloud*.



   d. In the *Switch EMS* dialog, in the *Invitation Code* field, copy and paste the invitation code obtained from

FortiSASE.



6. At this point, FortiSASE must be configured for endpoint management. See How can I configure FortiSASE for endpoint management? on page 323

I am an existing customer with a FortiClient Cloud deployment. What is the path to move to a FortiSASE deployment?

FortiSASE includes its own instance of EMS as part of the service, and it is required for proper orchestration of the solution. Therefore, customers with an existing FortiClient EMS solution will need to shift to using the FortiSASE instance of EMS.

Currently, the shift from an existing FortiClient Cloud to FortiSASE does not preserve FortiClient Cloud configuration because it will be replaced with configuration defined for FortiSASE after the process is completed. You must configure endpoint features supported in FortiSASE. See How can I configure FortiSASE for endpoint management? on page 323

The process below should allow endpoints to be shifted from FortiClient Cloud to FortiSASE without the need for a third-party endpoint management system.

This process should take one business week to complete. During this process, you cannot perform any provisioning of your new FortiSASE instance.

You must follow this process:

1. Contact your Fortinet Sales or Partner contact to perform one of these steps:
   - For an existing FortiClient subscription, a.k.a. the FortiClient FortiTrust license, to provide you with assistance with converting it to a FortiSASE user-based Standard, Advanced, or Comprehensive license
   - For an expired FortiClient subscription, to provide you assistance with purchasing a new FortiSASE user-based license.

   See the SASE and Zero Trust Ordering Guide.
2. Once you have a FortiSASE user-based license, to request the shift from using your FortiClient Cloud instance to using your FortiSASE instance for endpoint management, contact FortiCare Support Customer Service or open a new Customer Service ticket using the FortiCare Support Portal. The Customer Service team will assist you with these steps:
   a. Removing the FortiClient FortiTrust license from your FortiCloud root principal account (may take up to three business days).
   b. Creating a new Technical Support ticket to engage Fortinet technical teams to complete the request on the backend (may take up to two business days).
   c. Applying the new FortiSASE user-based license to your account.
3. Once the FortiClient Cloud license removal has completed, you will be informed via a Technical Support ticket update to either provision your FortiSASE instance on your own or to provide confirmation that Fortinet can provision your instance on your behalf.
4. After some time, the telemetry connection of each of the endpoints will be disconnected from FortiClient Cloud and will connect to the FortiSASE instance of EMS.

   a. Endpoints should connect to FortiSASE EMS.
   b. There is no need to restart FortiClient or the endpoint – simply wait for the next Telemetry synchronization event, typically, within 60 seconds.
5. At this point, FortiSASE must be configured for endpoint management. See How can I configure FortiSASE for endpoint management? on page 323

How can I configure FortiSASE for endpoint management?

Shifting from an on-premises FortiClient EMS or a FortiClient Cloud instance to FortiSASE does not preserve EMS configuration.

Some configuration settings from FortiClient EMS or FortiClient Cloud cannot be configured in FortiSASE because some FortiClient features are currently not supported in FortiSASE. See Supported FortiClient features.

Endpoint management features must be configured in the FortiSASE instance of EMS using the FortiSASE portal. This will require hands-on configuration time with the following options:

- If you want to perform the configuration themselves, follow these steps:
  a. Review FortiSASE documentation, namely Endpoints on page 244, for details on configuring endpoint management features.
  b. Purchase an Advanced or Comprehensive license and make use of *Assisted Onboarding*. See *FortiSASE Support Services* in the SASE and Zero Trust Ordering Guide.
  c. Perform the configuration in FortiSASE by logging in with the root principal email.
- If you want Fortinet to perform the endpoint management configuration in FortiSASE, purchase Fortinet Professional Services, and request either the **Advanced Deployment Service** or **Custom service engagement**. See *FortiSASE Support Services* in the SASE and Zero Trust Ordering Guide.

Appendix A - FortiSASE data centers

The following provides information about FortiSASE data centers or points of presence (PoPs) available through the FortiSASE Status page, global data centers list, and egress IP addresses feed. The following also provides information about the number of security data centers accessible per license.

Status page

To view real-time information on the current status of data centers, visit the FortiSASE Status page at https://status.fortisase.com and click the plus sign (+) next to *Fortinet Cloud Locations* or *Public Cloud Locations*.

Global data centers list

For a table of global data center information for FortiSASE, see Global data centers.

Egress IP addresses feed

A consumable feed of the FortiSASE egress IP addresses is available at https://portal.prod.fortisase.com/api/v1/public/egress/ips.

You can use this list in access control lists to allow access to internal applications from FortiSASE only.

For instances equipped with dedicated public IP addresses (via SKU addition, or through Advanced or Comprehensive licenses), the IP addresses associated with each FortiSASE security PoP are not included in the Egress IP API as they are customer-specific.

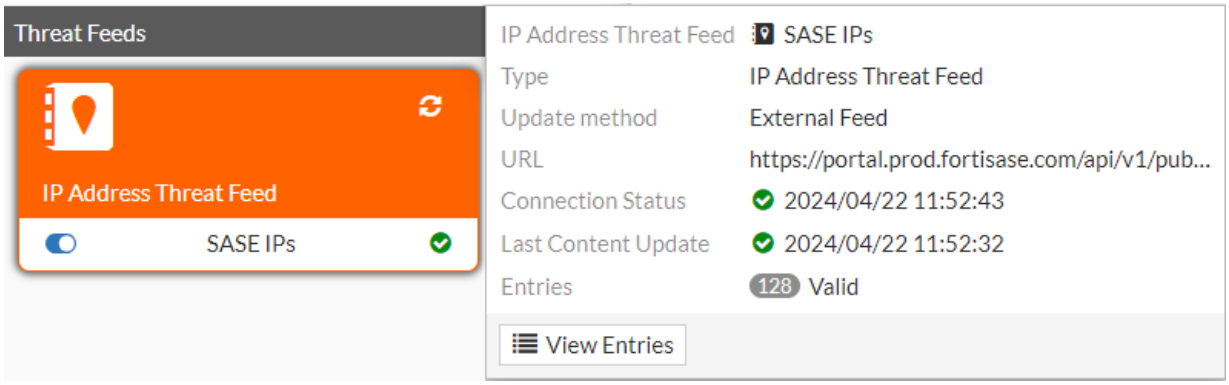
The egress IP addresses feed includes IP addresses for log forwarding and FortiSASE Endpoint Management Service. It is recommended that administrators of all instances, including those with dedicated IP addresses, use the egress IP addresses feed to allowlist traffic from both FortiSASE services based on their specific needs.

The following describes how to configure a threat feed using this feed in FortiOS. For information on threat feeds, see Threat feeds.

To create a threat feed using the FortiSASE egress IP address feed:

1. Go to *Security Fabric* > *External Connectors*.
2. Click *Create New*.

3. Under *Threat Feeds*, select *IP Address*.
4. In the *URL of external resource* field, enter https://portal.prod.fortisase.com/api/v1/public/egress/ips
5. Disable *HTTP basic authentication*.
6. Ensure that *Status* is enabled.
7. Configure other fields as desired, then click *OK*.
8. To confirm that you configured the feed correctly, wait until the GUI displays that the connection succeeded. Hover over the feed to see the connection status, last update time, and number of entries. You can use this feed to configure policies in FortiOS.



Number of security data centers accessible per license

The number of data centers with security capabilities that are accessible by remote users depends on the FortiSASE license tier and number of users, or user bands, applied to your FortiSASE instance. See the following table:

FortiSASE license	Number of security data centers accessible per user band		
	50-99 users	100-199 users	200+ users
Standard	2 to 4	2 to 4	2 to 4
Advanced			
Comprehensive	1	1 to 2	1 to 4
Not-for-Resale (NFR)	2 (50 users)	N/A	N/A
FortiAP 431F Promo Only	1 (no users)		

For the following license tiers, you can purchase access to additional security data centers with the corresponding FortiSASE Region Add-on license:

FortiSASE license	Region Add-on license
Standard	Fortinet Location Add-on
Advanced	
Comprehensive	Public Cloud Location Add-on

See the SASE and Zero Trust Ordering Guide.

Starting with FortiSASE 24.2.b, new instances with the FortiSASE Comprehensive license applied can select a combination of Fortinet and Public Cloud locations during initial provisioning. The maximum number of data centers accessible still depends on the number of users specified for the Comprehensive license and any region add-on licenses applied.

With the Region Add-on license and different FortiSASE license tiers, access to a maximum of 16 additional security data centers, or a maximum total of 20 security data centers, is possible.

During initial provisioning, you can select fewer security sites than the maximum you are entitled to. In this case, upon each login, the FortiSASE portal prompts you to select up to the maximum number of security sites.

If you decide to add additional security sites using this prompt, then FortiSASE allows for increasing the number of security sites without FortiCare Support. FortiSASE may experience up to 10 minutes of downtime when the entitlement is applied. If any errors occur, FortiSASE cannot automatically rollback without FortiCare Support.

For provisioning, you must select a minimum of two security sites for redundancy.

Appendix B - Beta

Features marked as "Beta" are available to use but may have constraints. These features are subject to continual improvements. Feedback is encouraged.

Appendix C - REST API

See the FortiSASE REST API reference on the Fortinet Developer Network.

Appendix D - VPN performance

Latency

High latency can have a significant impact on a user's observed internet performance.

When using FortiSASE, the goal is to ingress and egress traffic from the Fortinet network while introducing the smallest possible amount of network latency. FortiSASE achieves this by using high-quality internet service providers (ISP) and internet exchange points to minimize network hops.

In general, physical distance (e.g. the speed of light) and third party ISP routing to the last-mile introduce most network latency between the user and FortiSASE point of presence (PoP).

Evaluating and selecting PoPs for lowest latency

Prior to provisioning FortiSASE, evaluating which FortiSASE PoP will provide the lowest latency to your end users' locations and selecting these during provisioning is recommended.

To determine this, you can test the egress IP addresses in Appendix A - FortiSASE data centers on page 324 via `ping`, `traceroute`, or `mtr`.

Keep these latency thresholds in mind when evaluating these selections:

Latency level	Impact to performance	Latency (milliseconds (ms))
Ideal	Best performance	< 20 ms
Acceptable	Slightly impacted	20-60 ms
High	Moderately impacted	60-100 ms
Extreme	Significantly impacted	> 100 ms

Jitter and packet loss

Even if you observe ideal latency of under 20 ms in testing, packet loss and jitter can significantly impact performance.

- Jitter should be under 30 ms.
- Packet loss should be 0%.

You will observe significant degradation particularly for real-time communications (VoIP, video, and so on) beyond 30 ms of jitter and/or 1% packet loss.

Resolving increased latency with SSL VPN support for DTLS

While downloading a large file (100 MB or above) when using FortiSASE, you may observe increased latency (280 ms or above). SSL VPN support for DTLS is supported in FortiClient to resolve increase latency. See Supported FortiClient features.

Starting in 23.4.b, DTLS support is enabled by default for existing and new FortiSASE instances.

Appendix E - Maximum values

This topic provides minimum/maximum values for configuration settings in FortiSASE:

Setting	Minimum value	Maximum value
External feeds	0	20
Host addresses		20000
Secure private access service connections (hubs)		4
VPN and secure web gateway policies combined		10000
Zero trust network access connection rules		32000

www.fortinet.com