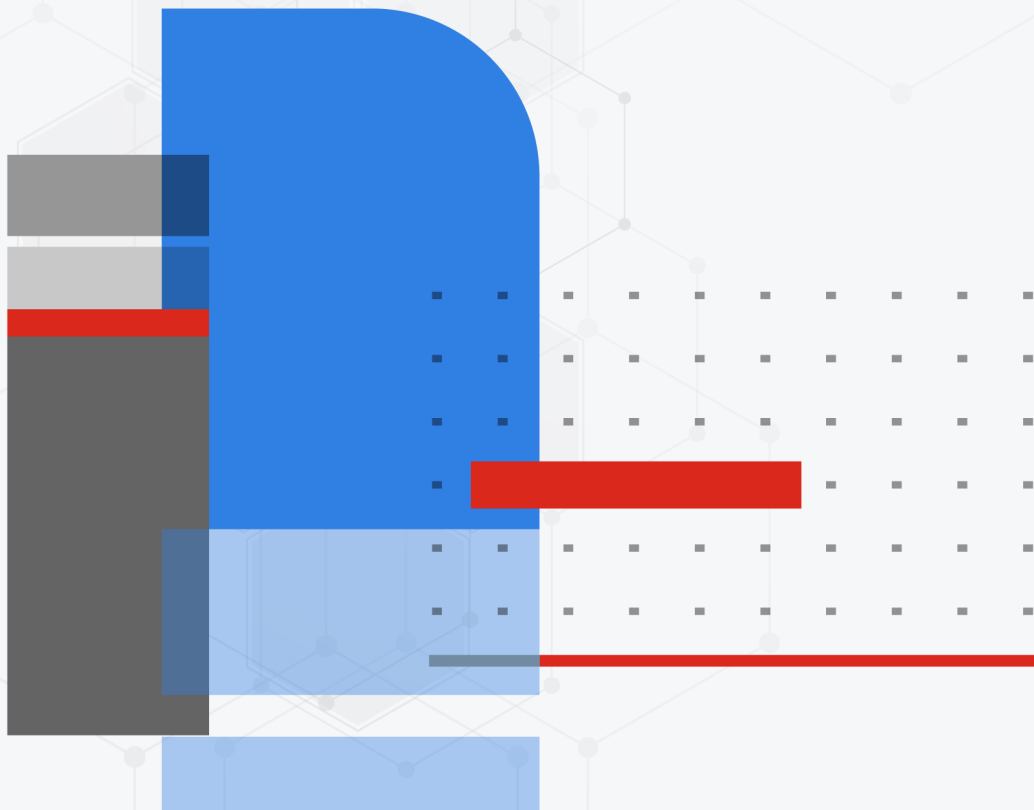




Administration Guide

FortiSASE 23.4.31



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



December 21, 2023

FortiSASE 23.4.31 Administration Guide

72-23431-938531-20231221

TABLE OF CONTENTS

Change log	6
Introduction	7
Endpoint mode	8
SWG mode	9
Signing in as an IAM user	9
System status notifications	10
Required services and ports	10
Supporting external IdP users	10
Dashboards	11
Adding a custom dashboard	11
Resetting all dashboards	12
Drilling down on vulnerabilities	12
FortiView monitors	13
Adding a custom monitor	14
Resetting all monitors	14
Monitoring thin-edge bandwidth usage	15
Thin-Edge	16
Edge devices	18
FortiExtender	18
Prerequisites	18
Viewing notifications for a new FortiExtender	21
Configuring FortiExtender as FortiSASE LAN Extension	21
FortiGate	29
Prerequisites	30
Viewing notifications for a new FortiGate	31
Configuring FortiGate as FortiSASE LAN Extension	31
FortiAP	36
Prerequisites	36
Viewing notifications for a new FortiAP	38
Configuring FortiAP as FortiSASE edge device	38
Network	46
Secure private access	46
Prerequisites	48
Configuring the FortiSASE security PoPs as the FortiGate hub's spokes	49
Verifying IPsec VPN tunnels on the FortiGate hub	68
Testing private access connectivity to FortiGate hub network from remote users	70
Verifying BGP routing on the FortiGate hub	70
Verifying private access traffic in FortiSASE portal	70
Verifying private access hub status and location using the asset map	72
Managed Endpoints	72
Management Connection button	73
Example: Confirming an endpoint is added to management by default	74
Example: Removing an endpoint from management	75

Example: Adding an endpoint to management after it was previously removed	76
Application inventory for managed endpoints	76
Digital Experience Monitoring	78
Configuration	81
DNS Settings	81
Split DNS Rules	82
Policies	86
Default VPN policies	86
Adding policies to perform granular firewall actions and inspection	86
Configuring a policy to allow traffic from the thin-edge LAN to FortiSASE for SIA	88
SWG Policies	89
Default SWG policies	89
Configuring a SWG policy	90
Security	92
Security profile groups	92
Web Filter	93
DNS Filter	107
Application Control With Inline-CASB	113
SSL Inspection	115
File Filter	117
Authentication Sources and Access	117
Configuring FortiSASE with an LDAP server for remote user authentication in endpoint mode	118
Configuring FortiSASE with an LDAP server for remote user authentication in SWG mode	122
Configuring FortiSASE with a RADIUS server for remote user authentication	125
Configuring FortiSASE with Entra ID SSO: SAML configuration fields	126
Configuring FortiSASE with Entra ID SSO in endpoint mode	127
Configuring FortiSASE with Microsoft Entra ID single sign on in SWG mode	131
Configuring FortiSASE with Okta SSO	132
Configuring FortiSASE with FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO	133
Searching user groups from SAML IdP	141
Testing SSO configuration from FortiSASE	145
Users	150
PKI	151
Endpoints	152
Profiles	152
Tagging	160
ZTNA Access Proxies	165
System	166
Certificates	166
HTML Templates	166
SWG Configuration	167
Analytics	169
Reports	169
Scheduling a report	169

Manually running a report	169
Report types	169
Logging	170
Forwarding logs to an external server	171
Log anonymization	172
Administrator Events	174
Log retention policy	174
Client onboarding	176
Managed endpoint client onboarding	176
SWG client onboarding	178
PAC file customization	178
Certificate installation	183
Proxy configuration	186
SWG Chrome extension and Chromebook support	190
Enterprise mobility management	194
Configuring Microsoft Intune integration with FortiClient (iOS)	194
MSSP portal	196
Prerequisites	196
Configuration workflow	196
Using the MSSP portal	197
Accessing the MSSP portal	198
Monitoring a tenant's instance	199
Managing a tenant's instance	200
Troubleshooting	201
Appendix A - FortiSASE data centers	202
Status page	202
Global data centers list	202
Egress IP addresses feed	202
Appendix B - Beta	204
Appendix C - REST API	205
Appendix D - VPN performance	206
Latency	206
Evaluating and selecting PoPs for lowest latency	206
Jitter and packet loss	206
Resolving increased latency with SSL VPN support for DTLS	207

Change log

Date	Change Description
2023-12-07	Initial release of 23.4.31.
2023-12-21	Updated Connecting FortiGate to FortiSASE using GUI and CLI on page 31 .

Introduction

FortiSASE is a software as a service-based 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 endpoints or 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.

FortiSASE offers the following modes:

Mode	Description
Endpoint	Endpoints connect to FortiSASE through an always-up VPN connection using FortiClient. In endpoint mode, you can also configure zero trust network access, an access control method that uses client device identification, authentication, and zero trust tags to provide role-based application access. See Endpoint mode on page 8 .
Secure web gateway (SWG)	Users configure FortiSASE as a SWG server in their browser. See SWG mode on page 9 .

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.

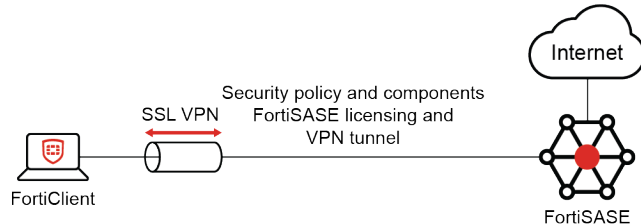
See [Service Organization Controls \(SOC2\) compliance standard](#).



Endpoint mode

In endpoint 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 [FortiSASE Ordering Guide](#).



The provisioning process for endpoint mode is as follows:

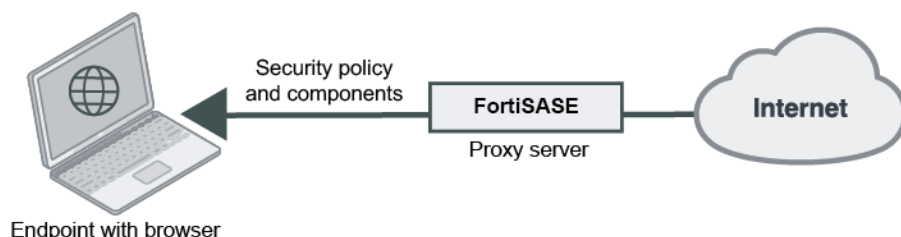
1. The administrator initializes the FortiSASE environment.
2. The administrator configures policies and security components in FortiSASE as desired, including configuring the desired policies. See [Adding policies to perform granular firewall actions and inspection on page 86](#).
3. The administrator 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 117](#) 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 170](#).

Endpoint 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 mode

In secure web gateway (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 SWG 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 mode and configuring the desired SWG policies. See [Configuring a SWG policy on page 90](#).
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 170](#).

Signing in as an IAM user

You can log in to FortiSASE as an 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 FortiCare subaccounts in cases where multiple users are accessing the FortiSASE customer portal.

To sign in as an IAM user:

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](#).

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.

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	443
IPsec VPN IKE	UDP	500
IPsec NAT-T	UDP	4500
CAPWAP	UDP	5246
SAML authentication	TCP	7831
Customer-specific secure web gateway port assignment	TCP	10445-50445

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 currently a limited beta feature in FortiCloud. If you require external IdP support for your FortiSASE instance, contact [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 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.

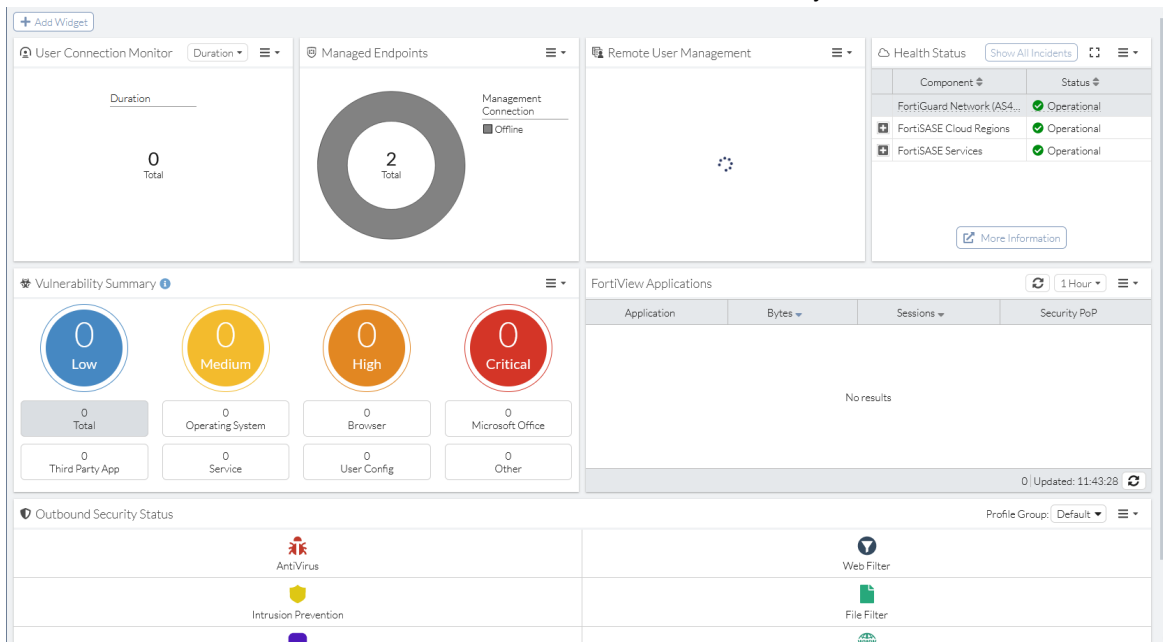
Adding a custom dashboard

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

To add a custom dashboard:

1. Under *Dashboards*, click +.
2. In the *Add Dashboard* pane, 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:

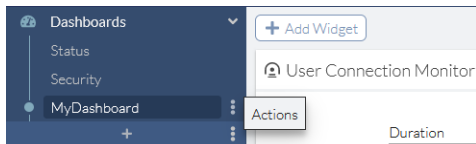


Resetting all dashboards

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 had 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.

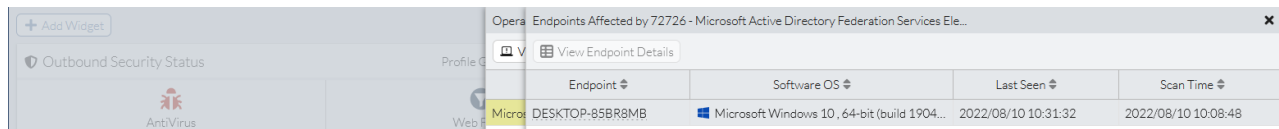
To drill down on vulnerabilities that belong to the same category:

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 is affecting, 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:

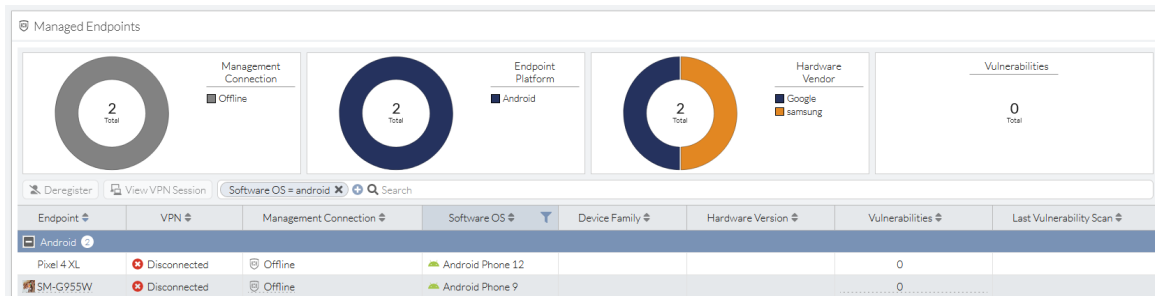
Dashboard	Usage
Sources	Displays sources by traffic volume and drilldown by source.
Thin-Edge	Displays Thin-Edge devices by traffic volume and drilldown by Thin Edge device.
Destinations	Displays destinations by traffic volume and drilldown by destination.
Applications	Displays applications by traffic volume and drilldown by application.
Cloud Applications	Displays cloud applications and drilldown by application.
Web Sites	Displays websites by session count and drilldown by domain.
Policies	Displays policies by traffic volume and drilldown by policy number.
Sessions	Displays sessions by traffic source.
VPN	Displays VPN connections by user.
Threats	Displays 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 the *Add Monitor* pane, select the desired FortiView or status monitor. In the example, you would select *Managed Endpoints*.
3. In the *Name* field, enter the desired name. Click *OK*.
4. You can further customize the monitor by applying filters or configuring the sort order on columns as desired. In the example, a filter has been applied to display only Android endpoints.

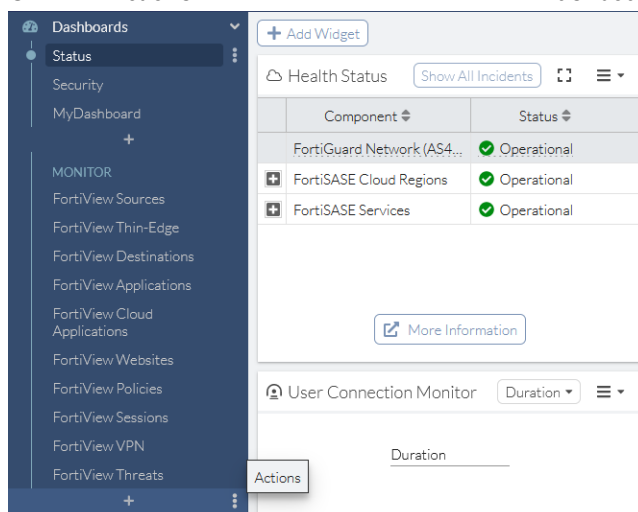


Resetting all monitors

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

To reset all dashboards:

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



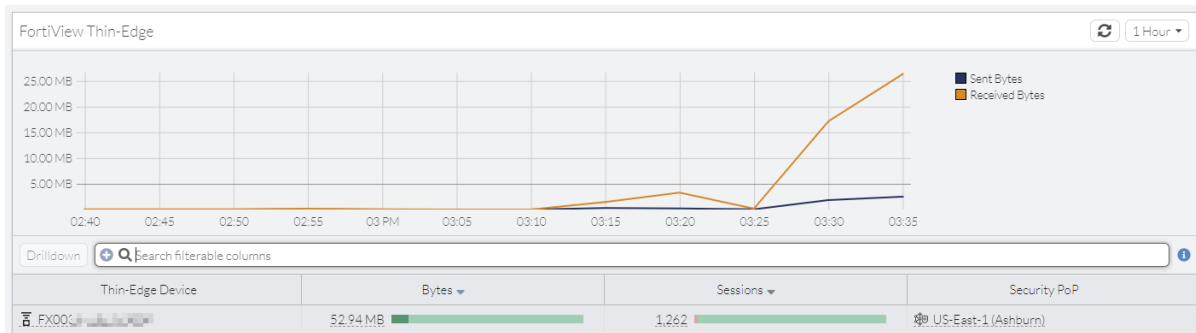
2. Select *Reset all Monitors*.
3. In the confirmation message, click *OK*.

Monitoring thin-edge bandwidth usage

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

To drill down on thin-edge bandwidth 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.

Sessions						
Search filterable columns Details						
Date/Time	User	Thin-Edge Device	Source IP	Destination IP	Application Name	Security
2022/05/02 16:15:57		FX000	10.251.0.3	172.253.115.97 (www.googletagmanag...	GoogleAnalytics	
2022/05/02 16:15:56		FX000	10.251.0.3	52.85.130.49 (b4fbc118aa4.cdn4.fort...	HTTPS.BROWSER	
2022/05/02 16:15:56		FX000	10.251.0.3	50.57.31.206 (uipglob.semasio.net)	HTTPS.BROWSER	
2022/05/02 16:15:56		FX000	10.251.0.3	172.253.115.156 (www.googleadservic...	SSL	
2022/05/02 16:15:56		FX000	10.251.0.3	142.250.81.194 (cm.g.doubleclick.net)	SSL	
2022/05/02 16:15:56		FX000	10.251.0.3	99.84.111.128 (cdn9.forter.com)	HTTPS.BROWSER	
2022/05/02 16:15:55		FX000	10.251.0.3	151.101.1.140 (alb.reddit.com)	Reddit	
2022/05/02 16:15:55		FX000	10.251.0.3	107.178.246.49 (pixel.tapad.com)	HTTPS.BROWSER	
2022/05/02 16:15:55		FX000	10.251.0.3	52.85.130.23 (www.mczbf.com)	HTTPS.BROWSER	
2022/05/02 16:15:55		FX000	10.251.0.3	142.251.16.113 (clients4.google.com)	HTTPS.BROWSER	
2022/05/02 16:15:49		FX000	10.251.0.3	151.101.2.132 (pt.ispot.tv)	HTTPS.BROWSER	
2022/05/02 16:15:49		FX000	10.251.0.3	151.101.2.102 (assets.nintendo.com)	HTTPS.BROWSER	
2022/05/02 16:15:49		FX000	10.251.0.3	23.47.49.89 (media-akam.licdn.com)	SSL	
2022/05/02 16:15:43		FX000	10.251.0.3	23.47.49.75 (media-akam.licdn.com)	SSL	
2022/05/02 16:15:41		FX000	10.251.0.3	151.101.2.137 (js-agent.newrelic.com)	HTTPS.BROWSER	
2022/05/02 16:15:41		FX000	10.251.0.3	35.244.142.80 (cdn.pdst.fm)	HTTPS.BROWSER	
2022/05/02 16:15:41		FX000	10.251.0.3	146.75.36.84 (s.pining.com)	SSL	
2022/05/02 16:15:41		FX000	10.251.0.3	3.8.8.8 (dns.google)	DNS	
2022/05/02 16:15:41		FX000	10.251.0.3	3.8.8.8 (dns.google)	DNS	

0% 2,812 | Updated: 16:16:24

OK Cancel

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 11](#).



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

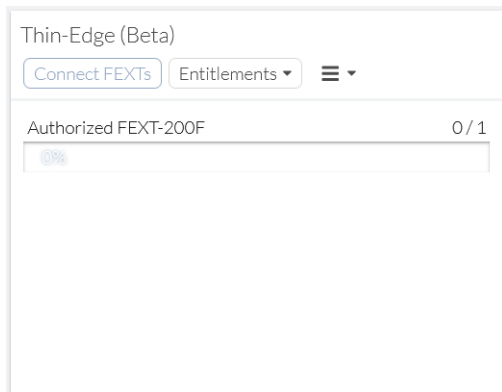


The FortiExtender-200F is the only supported model, and the *Entitlements* menu only shows authorized status and entitlement counts for this model.

2. Within the *Entitlements* view, you should be able to view the following status:

- a. Number of authorized FortiExtender devices
- b. Total number of entitlements

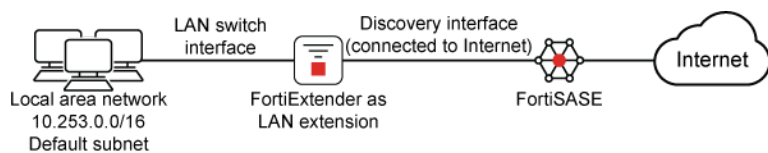
In the following screenshot, the *Thin-Edge* widget's *Entitlements* view displays zero authorized FortiExtender devices and one thin-edge management entitlement that has been registered. Therefore, in this case, only one FortiExtender device can be managed by FortiSASE.



Edge devices

FortiExtender

FortiSASE supports management and integration of a FortiExtender configured as a LAN extension. A FortiExtender with the LAN extension configuration allows a micro-branch deployment. A micro-branch 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.



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

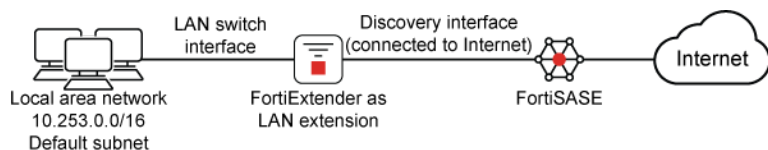
You must register FortiExtender devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

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:



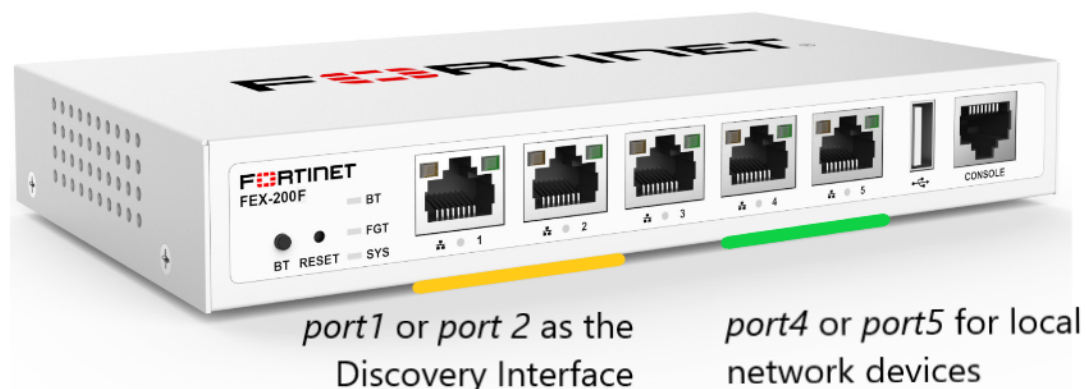
By default, using DHCP, FortiSASE dynamically assigns IP addresses to devices connected to the local network of the FortiExtender, that is, the LAN switch interface.

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 19](#) 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.

Physical Port

Cancel

Save

Name*		Type	
port1		physical	
Mode		Role	
☐ dhcp ☒ static		☐ lan ☒ wan	
Allow Access		Distance	
☒ ping ☒ ssh ☐ telnet ☐ http ☒ https ☐ snmp		51	
IP*	Gateway	MTU Override	MTU
192.168.2.1/24	192.168.2.254	☒ enable ☐ disable	1500
Status	As DHCP Server		
☒ up ☐ down	☐		
VRRP Status			
☐ enable ☒ disable			

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:

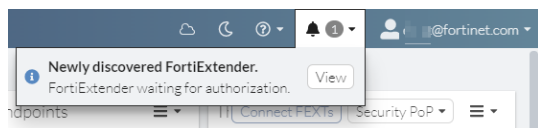
```
config system interface
  edit <port>
    set mode { dhcp | static }
    set ip <interface IP address/subnet>
    set gateway <gateway IP address for static IP address configuration>
  next
end
```

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
```

Viewing notifications for a new FortiExtender

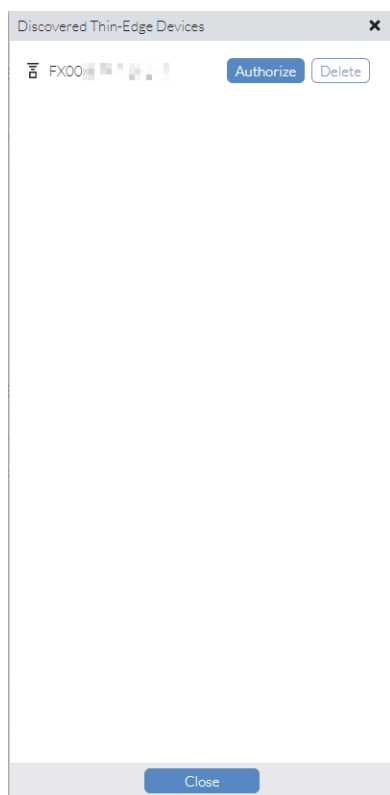
When a new FortiExtender powers on, the bell icon in the header displays a notification about the new device. In this example, the 1 beside *Network* in the left navigation pane also indicates the new device.



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

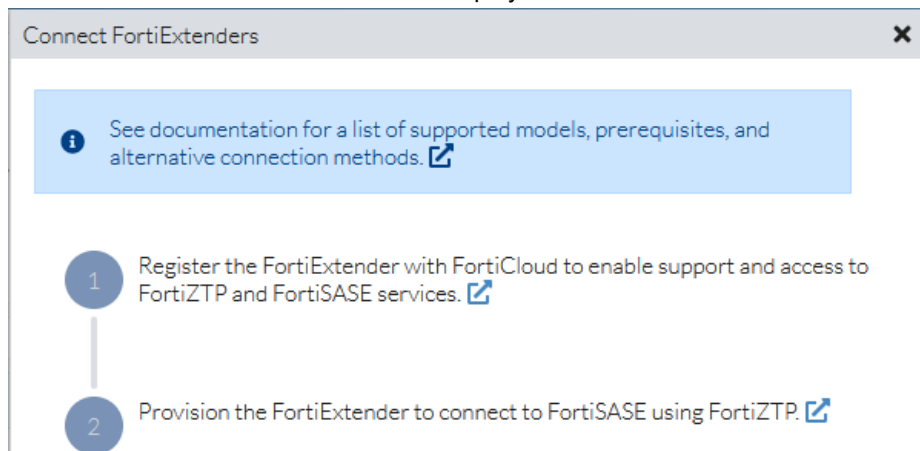
In *Edge Devices > FortiExtenders*, you can authorize, deauthorize, and delete FortiExtenders:

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.



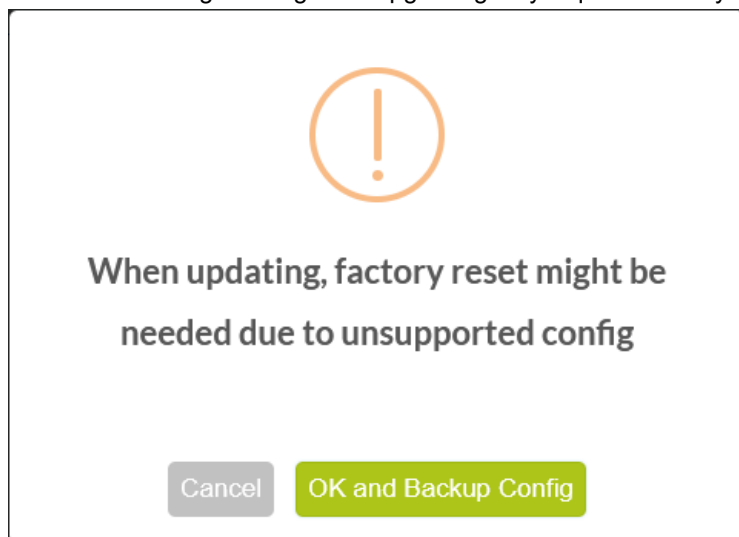
In addition to the instructions in the *Connect FEXTs* dialog, you generally must perform these preliminary steps to ensure proper connectivity:

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`:

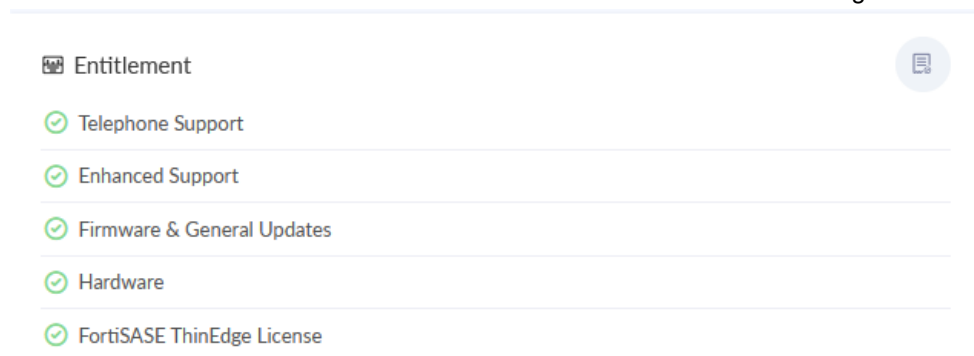
```
FX200F # execute factory-reset
The operation will do factory reset and then reboot the system!
Do you want to continue? (y/n)y
```

A reboot occurs as part of the factory reset process.

To register FortiExtender and FortiSASE license on FortiCloud:

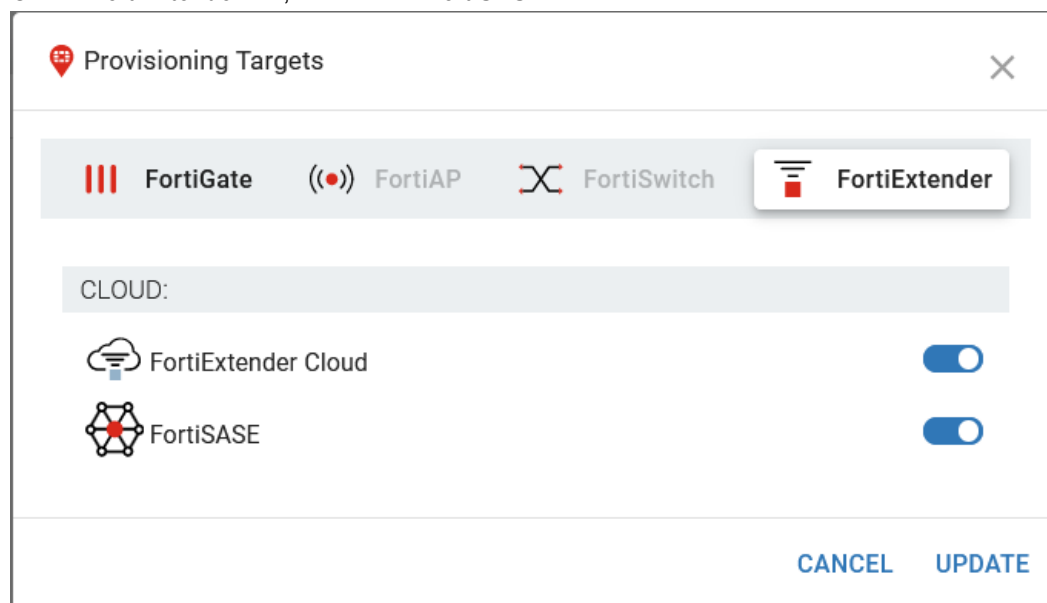
1. Sign in to your [FortiCloud account](#).
2. Go to *Products* and click the *Register More* button.
3. In the *Register Product* dialog, in the *Registration Code* field, enter the FortiExtender serial number and follow the dialogs to complete registering the FortiExtender. For details on registering 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 28](#) 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 21](#) 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`.

VPN USER SINGLE SIGN ON (SSO)

1

2

Configure Identity Provider
Configure Service Provider

i On your Identity Provider, add FortiSASE as a Service Provider using the following information.

Base URL	https://turbo-a1p0hv3p.edge.prod.fortisase.com	
Entity ID	https://turbo-a1p0hv3p.edge.prod.fortisase.com/remote/saml	
Assertion Consumer Service (ACS) URL <i>i</i>	https://turbo-a1p0hv3p.edge.prod.fortisase.com/remote/saml	

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*.

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



Management Settings

, The change of property "discovery-type" or 11
"local"->"mode" setting may result in system reboot!

Cancel

OK

- 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*.

Controller Infomation		
 FortiGate	Serial Number	FGVMPGTM[REDACTED]
	FGT IP	206.4[REDACTED]
	Local IP	172.5[REDACTED]
	Status	Connected

To connect a FortiExtender to FortiSASE via the CLI:

The following commands are adapted from [FortiExtender LAN extension in public cloud FGT-VM](#).

- 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 : FGXXXXXXXXXXXXXXXXXX
  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 22](#).
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 23](#).
 - For details on performing a factory reset using the FortiExtender CLI, see [To factory reset the FortiExtender from the CLI: on page 23](#).
 - 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 18](#).
4. Connect your Internet connection to port 1 and local LAN to ports 4-5. See [Network topology on page 18](#).



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

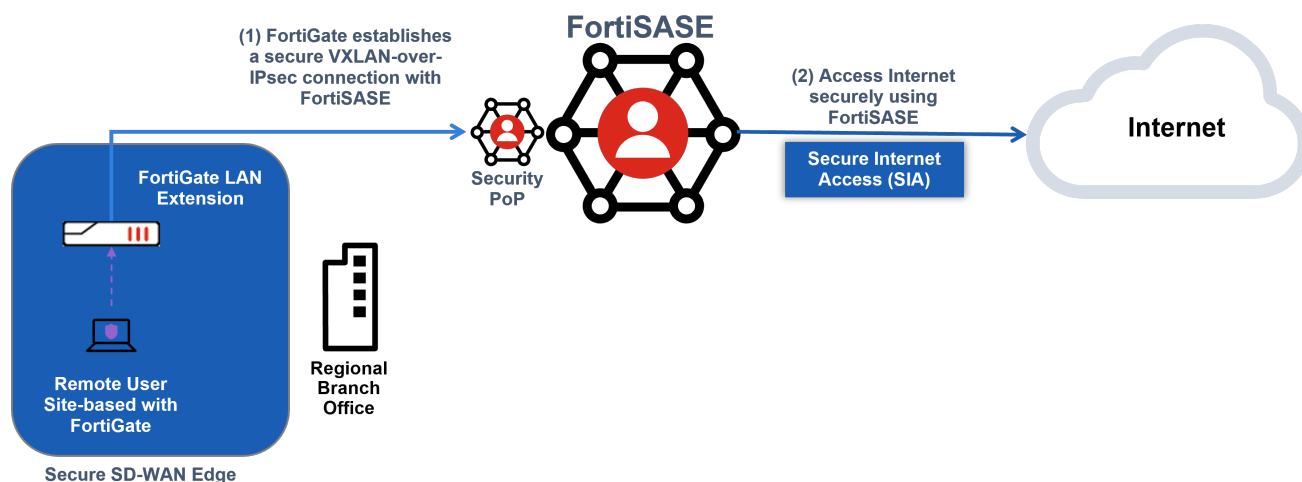


FortiGate SD-WAN as a secure edge is a controlled General Availability feature that requires a separate FortiSASE subscription license per FortiGate. All FortiGate F-series and G-series desktop platforms running FortiOS 7.4.2 and above are capable of supporting FortiSASE Secure Edge connectivity.

Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiGate. To enable this feature for your tenant after it has been licensed accordingly, the FortiSASE security PoPs must run a feature release environment. If you require this support for your FortiSASE instance and already have the proper licenses, contact [FortiCare Support](#).

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), the endpoints only need to be configured in their IP settings to forward traffic to the FortiGate as the default gateway.

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 endpoint do not require explicit web proxy settings to be configured.



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

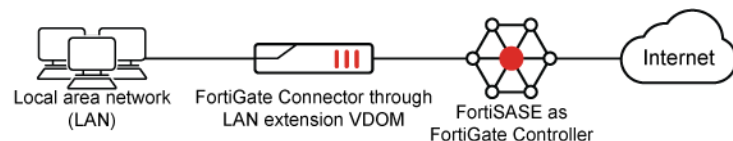
You must register FortiGate devices used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE before using this feature.

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.

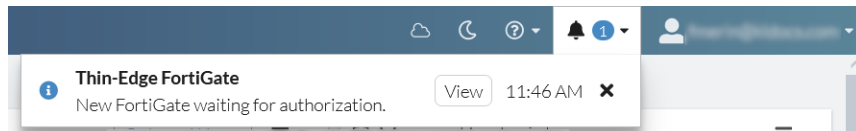
Connecting and logging into the FortiGate

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](#).

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 GUI and CLI

For details on configuring the FortiGate secure edge to connect to FortiSASE using GUI or CLI, see [FortiGate LAN extension](#). Follow steps related to configuring the FortiGate Connector because the FortiGate secure edge fulfills the role of a FortiGate Connector while the FortiSASE fulfills the role of the FortiGate Controller.

Before configuring the FortiGate Connector, 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`.

VPN USER SINGLE SIGN ON (SSO)

1 Configure Identity Provider

2 Configure Service Provider

i On your Identity Provider, add FortiSASE as a Service Provider using the following information.

Base URL

Entity ID

Assertion Consumer Service (ACS) URL **i**

To configure the FortiGate Connector using the CLI:

1. Enable multi-VDOM mode from the CLI:

```
config system global
    set vdom-mode multi-vdom
end
```

2. Verify that the FortiExtender setting is enabled in the global VDOM:

```
# config global
# show full system global | grep fortiextender -f
...
    set fortiextender enable
...
```

3. Create a new LAN extension VDOM (named `lan-ext` arbitrarily in the example below), configuring the LAN extension controller address to be the FortiSASE domain name determined above.

```
config vdom
    edit lan-ext
        config system settings
            set vdom-type lan-extension
            set lan-extension-controller-addr turbo-a1p0hv3p.edge.prod.fortisase.com
            set ike-port 4500
        end
    next
end
```

4. Move interfaces from the root VDOM to the new LAN extension VDOM, setting the appropriate WAN and LAN roles.
 - You will need to ensure that any references such as firewall policies or firewall objects have been deleted before moving an interface to a new VDOM. See [Finding object dependencies](#).
 - If interfaces are already part of a hardware switch, then you will need to remove them from the hardware switch to make them available for the new VDOM. See [Hardware Switch](#).

For example, to move WAN1 and internal1 to the `lan-ext` VDOM and set their roles appropriately from the global VDOM:

```

config global
    config system interface
        edit WAN1
            set vdom "lan-ext"
            set role wan
        next
        edit internal1
            set vdom "lan-ext"
            set role lan
        next
    end
end

```

5. For the WAN interface within the LAN extension VDOM, edit the interface and ensure that Security Fabric Connections are allowed:

```

config vdom
    edit lan-ext
        config system interface
            edit WAN1
                set allowaccess ping fabric
            next
        end
    next
end

```

This configuration assumes you have already configured the WAN and LAN interfaces with static IP addresses or configured them to use DHCP accordingly.

6. (Optional) If your LAN extension VDOM is not configured as the management VDOM and you require a custom DNS server to resolve the FortiGate Controller hostname, you must configure the VDOM DNS settings within the VDOM using these commands:

```

config vdom
    edit ext
        config system vdom-dns
            set vdom-dns enable
            set primary 1.2.3.4
            set secondary 2.3.4.5
        end
    next
end

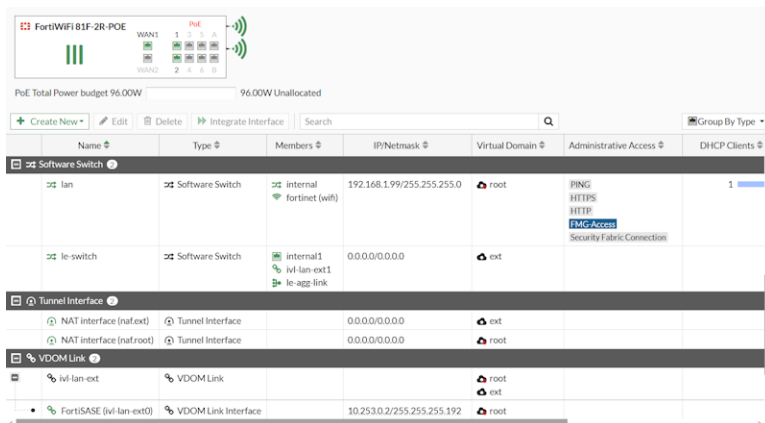
```

7. After the LAN extension VDOM connects to FortiSASE, observe from the global VDOM under *Network > Interfaces*:

- A VDOM link *ivl-lan-ext* is created.
- The VDOM link interface in the LAN extension VDOM (*ivl-lan-ext1*) is part of the *le-switch* LAN extension software switch. Network connectivity to the FortiGate Controller (that is, to FortiSASE) is achieved through the software switch.
- The VDOM link interface in the traffic (root) VDOM (*ivl-lan-ext0*) has obtained an IP address dynamically from the FortiGate Controller.

The traffic VDOM can be used to:

- Apply application steering to the local internet connection or to FortiGate Controller network (FortiSASE) using SD-WAN.
- Apply local security features for traffic egressing the local internet connection, such as antivirus, intrusion prevention security (IPS), application control, and web filtering, by creating a firewall policy with *ivl-lan-ext0* as the destination interface.



8. Create a firewall policy with *ivl-lan-ext0* as the destination and *lan* as the source within the traffic VDOM to allow local traffic from the FortiGate Connector to access the internet through the FortiGate Controller (FortiSASE):

```
config firewall policy
  edit 1
    set name "traffic-VDOM-to-FortiSASE"
    set srcintf "lan"
    set dstintf "ivl-lan-ext0"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

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 30](#).
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 30](#).
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*.

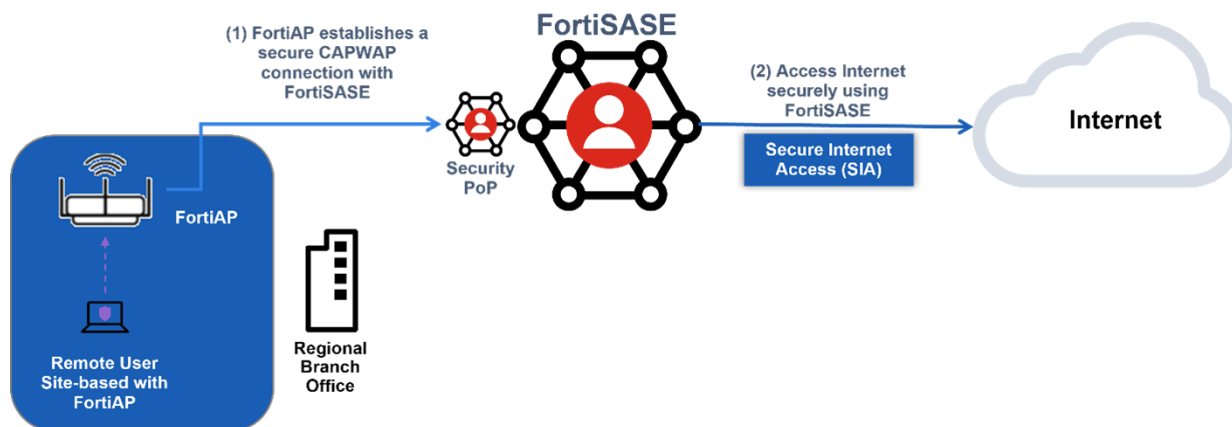
FortiAP



FortiAP edge device support is a controlled General Availability feature that requires a separate FortiSASE subscription license per FortiAP. FortiAP 231F and 431F devices running FortiAP firmware 7.2.4 and above are supported.

Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiAP. To enable this feature for your tenant after it has been licensed accordingly, the FortiSASE security PoPs must run a feature release environment. If you require this support for your FortiSASE instance and already have the proper licenses, contact [FortiCare Support](#).

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.



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

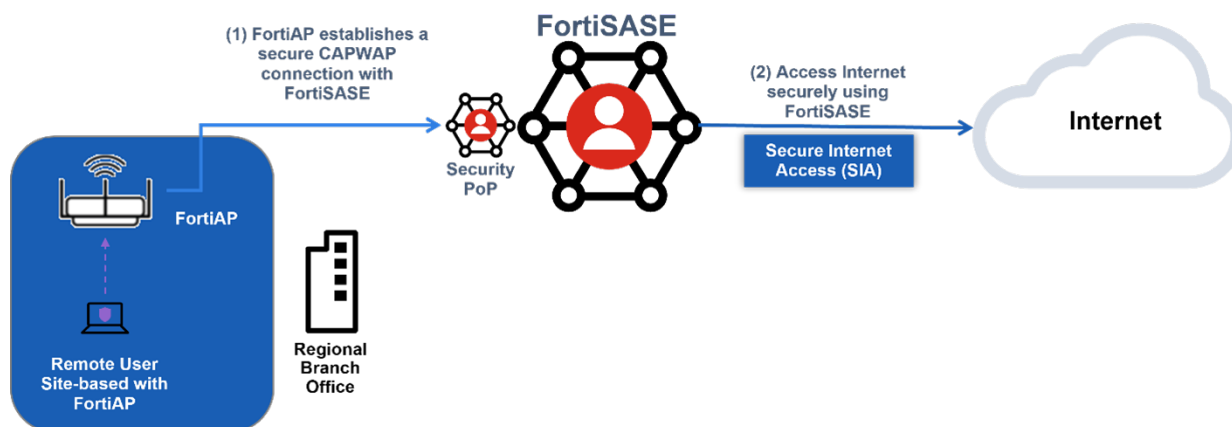
You must register FortiAP devices to the same FortiCloud account used to log into FortiSASE before using this feature.

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.

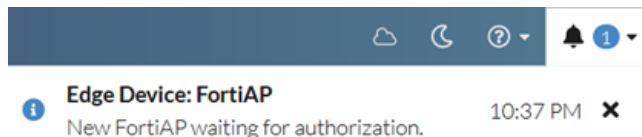
2. Configure the computer to be on the same subnet as the FortiAP by changing its IP address to 192.168.1.1 and the netmask to 255.255.255.0.
3. Access the GUI or CLI using 192.168.1.2:
 - a. In a web browser, go to the default FortiAP web GUI address: `https://192.168.1.2`.
 - b. Using SSH, go to 192.168.1.2.
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:

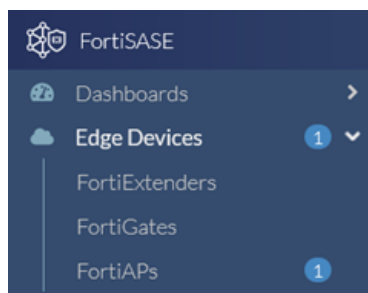
1. Ensure that the FortiAP is booted up.
2. Use a pin to push and hold the reset button for five to ten seconds. FortiAP reboots and then enters Configuration mode. FortiAP starts to broadcast an open security SSID `FAP-config-<serial-number>`, for example `FAP-config-FP421F0000000000`.
3. Access the 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.

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 GUI or CLI on page 39](#)
- [Troubleshooting a FortiAP that FortiSASE does not see on page 40](#)
- [Managing FortiAPs on page 41](#)

- [Editing a FortiAP profile on page 42](#)
- [Creating a FortiAP profile and applying it to a FortiAP on page 44](#)
- [Creating an SSID on page 44](#)

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

1. Connect the FortiAP to FortiSASE using GUI or CLI.
2. Log into FortiSASE and view notifications confirming that FortiSASE sees the FortiAP.
3. Authorize the FortiAP.
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 all SSIDs or selected SSIDs.

Connecting a FortiAP to FortiSASE using GUI or CLI

You can connect a FortiAP to FortiSASE using the FortiAP GUI or CLI.

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`.

VPN USER SINGLE SIGN ON (SSO)

1 ————— 2

Configure Identity Provider Configure Service Provider

i On your Identity Provider, add FortiSASE as a Service Provider using the following information.

Base URL

Entity ID

Assertion Consumer Service (ACS) URL **i**

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.

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 37](#).
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 37](#).
3. Ensure that after you make configure the FortiSASE domain name in the FortiAP GUI or CLI in Configuration mode, you reboot the FortiAP.
4. 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
```

```

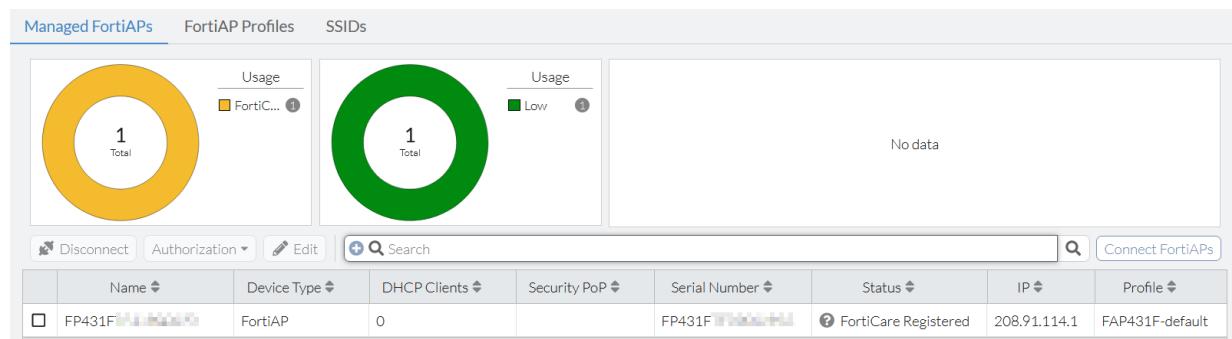
...
ACS 0 info
  wcha info           : mode=0 max=10 wait=10 peer_cnt=0
  acPri              : 1
  fsm-state          : RUN 768
  ac-ip-addr         : 154.52.4.72:5246,5247      DNS
  ac-name            : FGVMABCD00000EFG
  ...
  data-chan-sec-oper : ipsec-sn
  ...

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            :
  ...

```

Managing FortiAPs

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



From this page, you can perform these tasks:

Authorizing a FortiAP



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

To authorize a FortiAP:

1. Go to *Edge Devices > FortiAPs* 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*.

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.

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 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: <i>Disabled</i>: radio is disabled. <i>Access Point</i>: 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.
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. <i>Three Channels</i>: automatically selects channel 1, 6, and 11. <i>Four Channels</i>: automatically selects channels 1, 4, 8, and 11. <i>Custom</i>: select custom channels.
Channels	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in <i>Band</i> . By default, for 5 GHz radios

Field	Description
	all available channels are enabled.
Transmit Power Mode	Select how you want to determine transmit power: <i>Percent</i>: transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device. <i>dBm</i>: transmit power is setting using a dBm value. <i>Auto</i>: 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.
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.

General SSID settings

Field	Description
Name	Enter a name for the SSID interface.
Traffic Mode	<i>Tunnel</i> — (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.

Field	Description
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. • <i>WPA2 Personal</i>: WPA2 is WiFi Protected Access version 2. Users use a pre-shared key (password) to obtain access. • <i>WPA2 Enterprise</i>: similar to WPA2 Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password. • <i>WPA3 Enterprise Only</i>: 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 <i>Mode</i> is <i>WPA2 Personal</i> . Preshared key must be 8 to 63 characters long.
Authentication	Available only when <i>Mode</i> is <i>WPA2 Enterprise</i> or <i>WPA3 Enterprise Only</i>. Select one of the following: • <i>RADIUS Server</i>: select the RADIUS server that will authenticate the clients. • <i>User Groups</i>: select the local user group(s) that can authenticate.

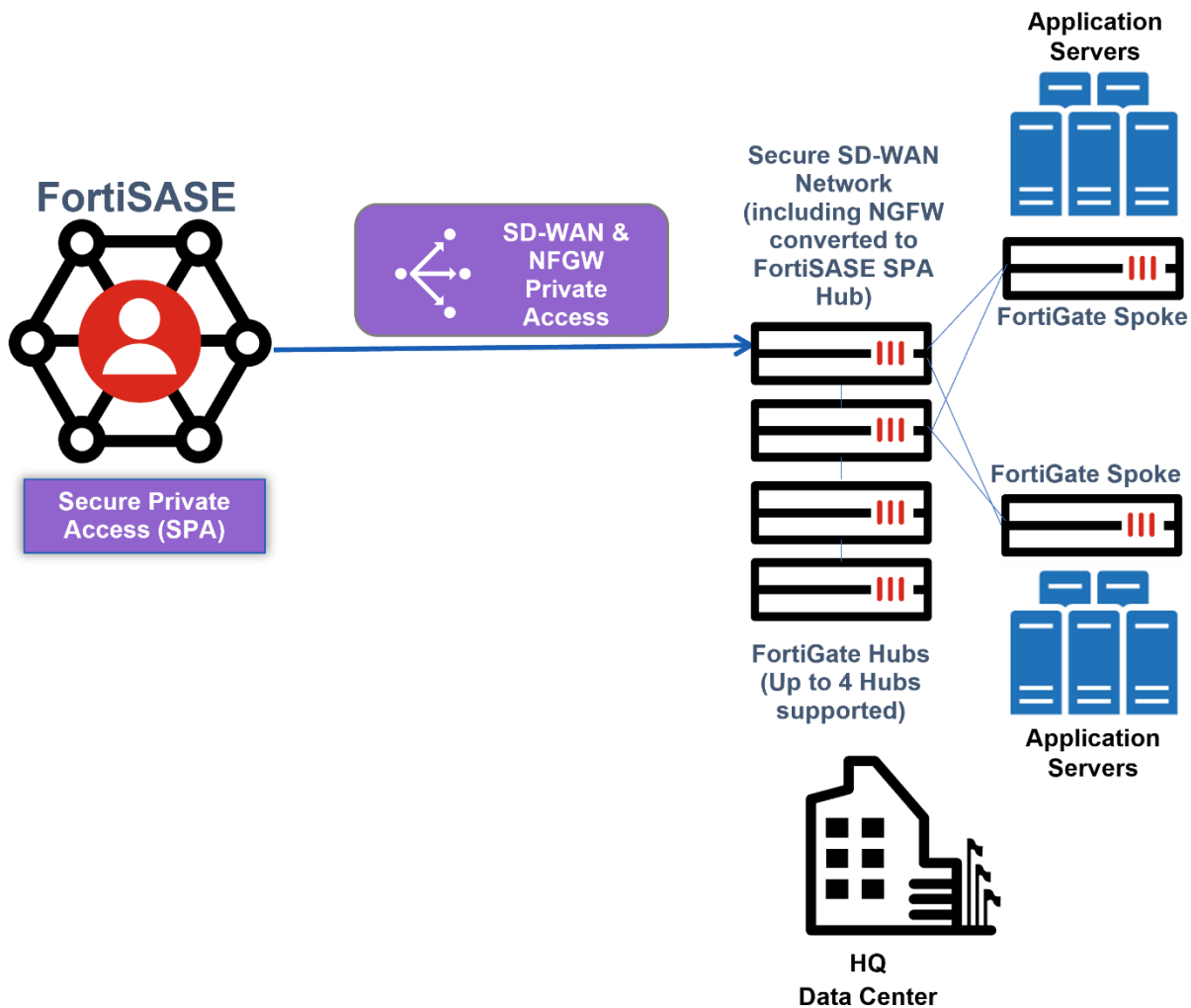
Network

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

Dashboard	Description
Asset Map	Displays the geographical location of assets, including servers, on a global map. Also indicates which server has logging enabled.
Thin-Edge	View, authorize, deauthorize, and delete FortiExtender devices.
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.

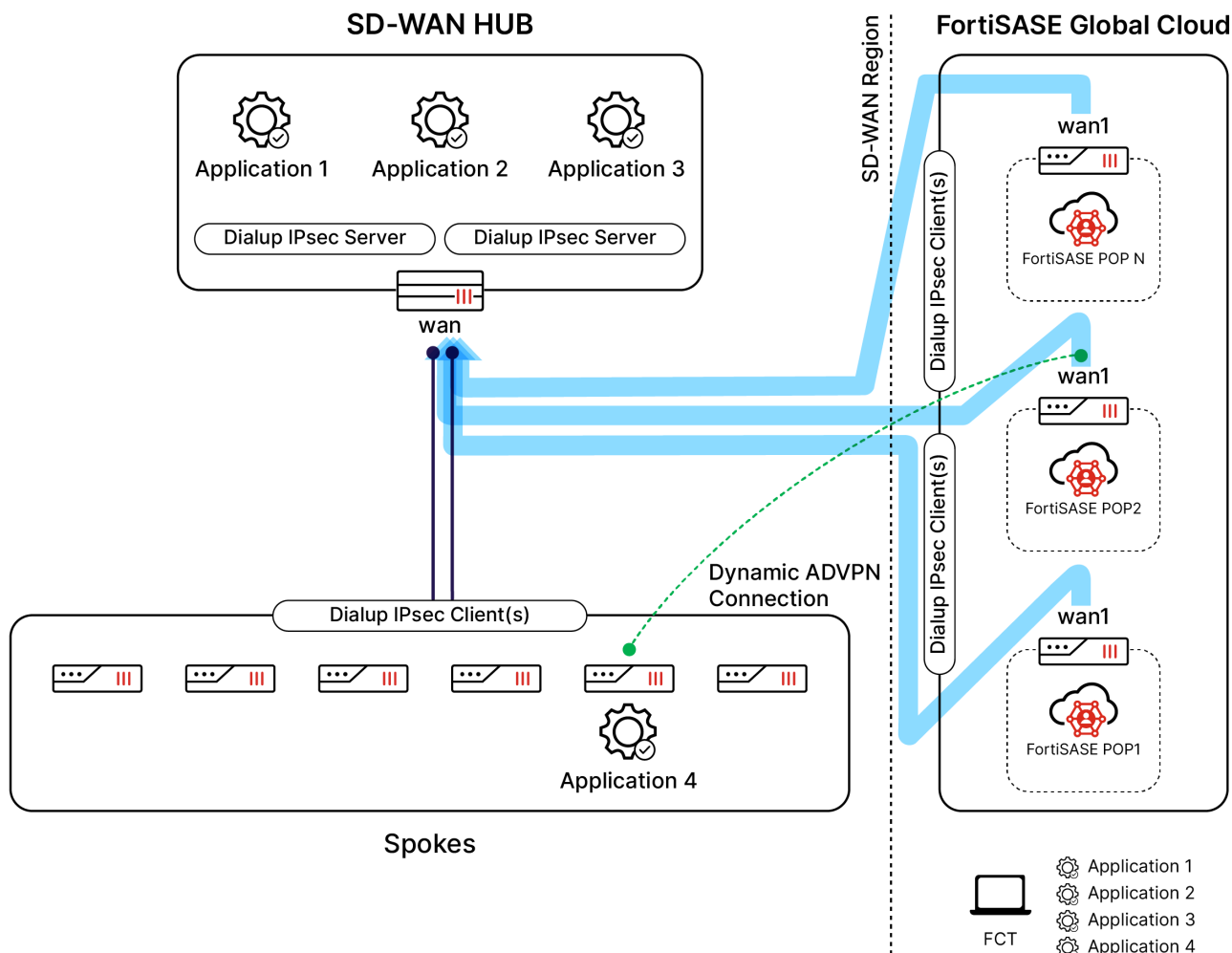
Secure private access

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 points of presence 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. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

See [Routing design methods](#).

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 Service Connection license



Secure private access (SPA) Service Connection license enforcement takes effect with the FortiSASE 23.3 release in Q3 2023. Customers who have not already enabled SPA at that time are required to purchase a license. See the FAQ in the [FortiSASE Ordering Guide](#).

A single SPA Service Connection license is required per FortiGate and allows inbound connectivity to the licensed device from all remote user and branch locations.

- FortiGate desktop platforms are recommended as a single next generation firewall location only.
- FortiGate 100F series and above recommended for an SD-WAN hub.

See the [FortiSASE Ordering Guide](#).

Network restrictions

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

- 10.8.0.0/16
- 10.16.0.0/16
- 100.64.0.0/10
- 10.252.0.0/16
- 10.253.0.0/16

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



Before configuring the Secure Private Access settings in the FortiSASE portal, to ensure proper secure private access (SPA) functionality, you must ensure that the FortiGate hub conforms to the deployment details (topologies, configuration settings) covered in the specific 4-D FortiSASE SPA deployment guide corresponding to your SPA use case as [Prerequisites on page 48](#) 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 50](#).
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 52](#).



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

Configuring network configuration

Before proceeding with configuring hubs or service connections, you must configure common SPA network configuration used by all service connections.



Only a single BGP routing design method can be used for all hubs and spokes. They cannot be mixed.

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 Connection* 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 performs input validation 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 on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them. See Routing design methods.	BGP per overlay

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 security PoPs. /28 is the minimum subnet size. For <i>BGP on loopback</i> , you must configure this subnet as a neighbor range in the hub BGP settings.	10.20.1.0/24
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. • 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.	Hub health and priority
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 ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.8.0.0/16
- 10.16.0.0/16
- 100.64.0.0/10
- 10.252.0.0/16
- 10.253.0.0/16



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.



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.

Service Connections **Network Configuration**

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design
BGP Router ID Subnet
Autonomous System Number (ASN)
BGP Recursive Routing
Hub Selection Method

BGP per overlay BGP on loopback

☒

Hub Health and Priority
BGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

Health Check IP

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



The corresponding BGP routing design method was configured in the *Network Connection* 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 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
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 <i>Pre-shared key</i> (default) and <i>Certificate</i> .	Pre-shared key
Pre-shared key (PSK)	When <i>Authentication Method</i> is configured as <i>Pre-shared key</i> , define the hub PSK.	mysecretkey
PKI User	When <i>Authentication Method</i> is configured as <i>Certificate</i> , 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 <i>+Create</i> or via <i>Configuration > PKI</i> , then select it here.	mypeer
Certificate	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via <i>System > Certificates</i> as a <i>Local Certificate</i> .	Fortinet_Factory
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.10.10.253

Network attributes	Description	Example
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 ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.8.0.0/16
- 10.16.0.0/16
- 100.64.0.0/10
- 10.252.0.0/16
- 10.253.0.0/16



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.

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:

#	Name	Configuration State	Remote Gateway	BGP Peer IP	Network Overlay ID
1	DC1	Success			11
2	DC2	Success			12



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
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 <i>Pre-shared key</i> (default) and <i>Certificate</i> .	Pre-shared key
Pre-shared key (PSK)	When <i>Authentication Method</i> is configured as <i>Pre-shared key</i> , define the hub PSK.	mysecretkey
PKI User	When <i>Authentication Method</i> is configured as <i>Certificate</i> , 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 <i>+Create</i> or via <i>Configuration > PKI</i> , then select it here.	mypeer
Certificate	When <i>Authentication Method</i> is configured as <i>Certificate</i> , select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via <i>System > Certificates</i> as a <i>Local Certificate</i> .	Fortinet_Factory
ADVPN Route Tag	For <i>BGP on loopback</i> 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	10.10.10.253

Network attributes	Description	Example
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 ranges are reserved for FortiSASE internal usage, note the following network restrictions, and ensure your network configuration does not overlap with them:

- 10.8.0.0/16
- 10.16.0.0/16
- 100.64.0.0/10
- 10.252.0.0/16
- 10.253.0.0/16



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.

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:

Health and VPN Tunnel Status

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

DC1

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☒	San Jose - California - U...	Up	Up	Established

< 1 >

DC2

View Learned BGP Routes

	Region	Health Check IP Status	VPN Tunnel	BGP Peering State
☐	San Jose - California - U...	Up	Up	Established

< 1 >

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:

Learned BGP Routes

Search

Prefix	Next Hop	Learned From
10.251.1.1/32	0.0.0.0	0.0.0.0
10.100.99.0/24	10.251.1.253	10.251.1.253
192.168.111.0/24	10.251.1.253	10.251.1.253

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.

Update Service Connection Priorities

i PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▾ San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC1	P1 (Highest Priority)
☐	DC2	P1 (Highest Priority)

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:

Update Service Connection Priorities

i PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▾ San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC1	P2
☐	DC2	P1 (Highest Priority)

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

Update Service Connection Priorities

i PoPs will choose the service connection with the highest priority that satisfies the SLA to forward traffic.

Set Priority ▾ San Jose - California - USA ▾

☐	Name	Priority ▲
☐	DC2	P1 (Highest Priority)
☐	DC1	P2

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:

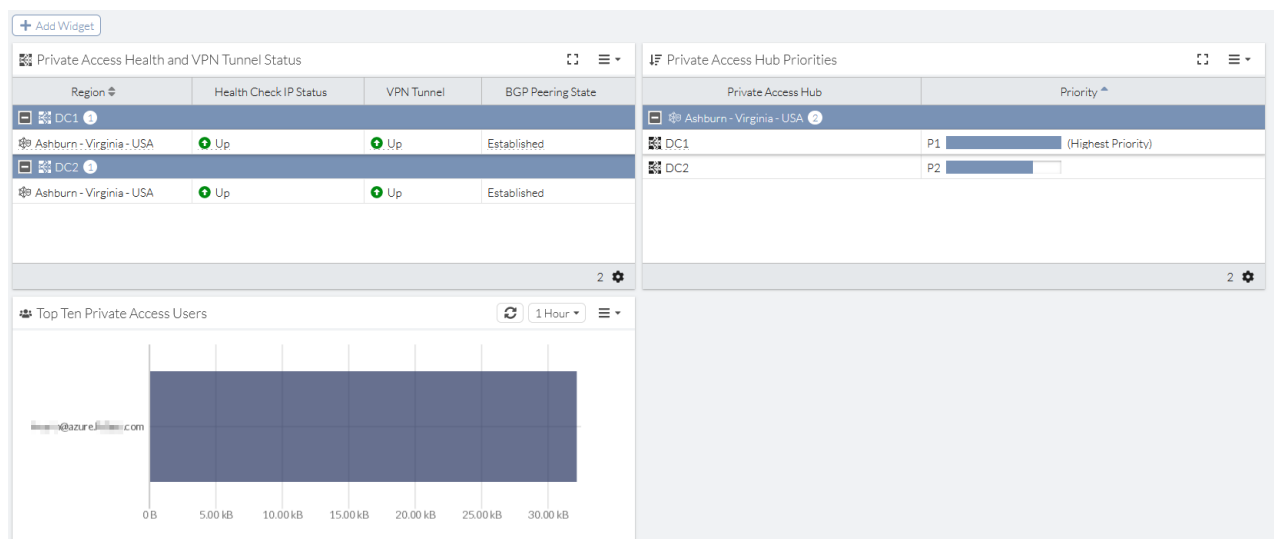
1. Go to *Network > Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

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:



Verifying private access policy configuration

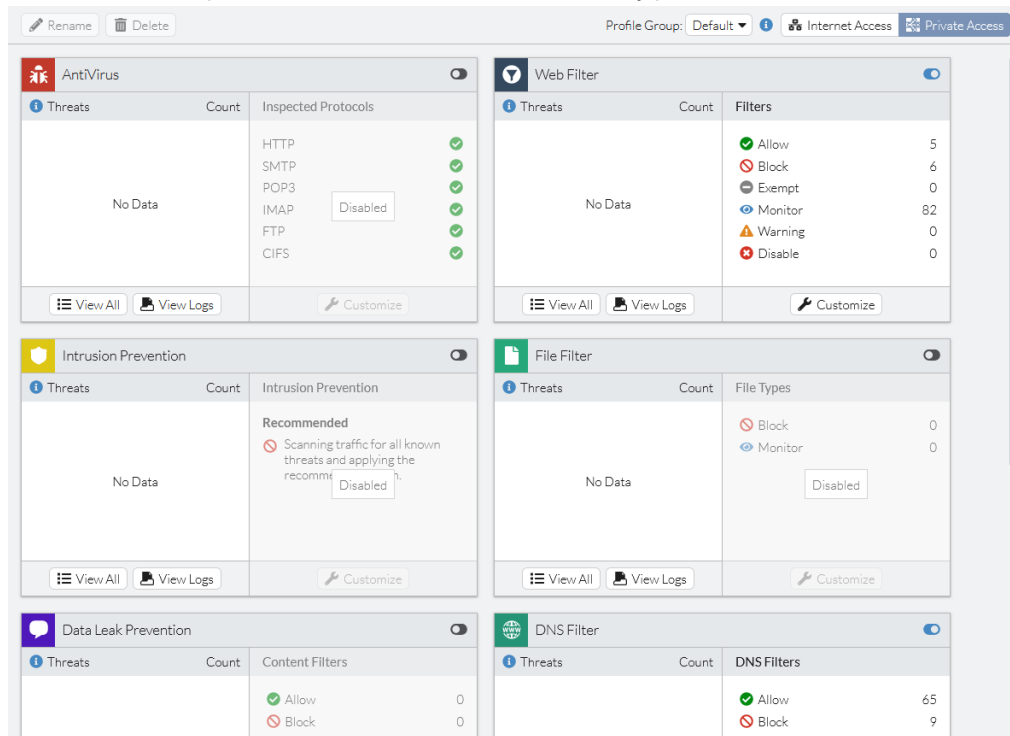
To verify private access policy configuration:

1. Go to *Configuration > Traffic > Policies*.
2. Click *Secure Private Access*.
3. View the configured private access policy.

Configuring a private access security profile

To configure a private access security profile:

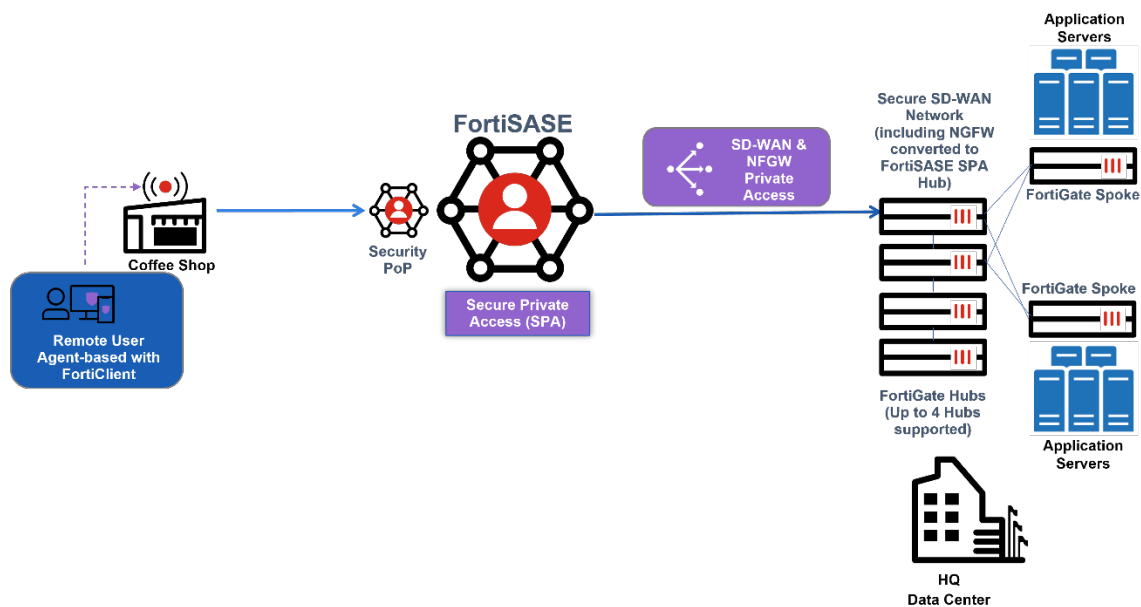
1. Go to *Configuration > Traffic > Security*.
2. In the top right corner, click *Secure Private Access*.
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



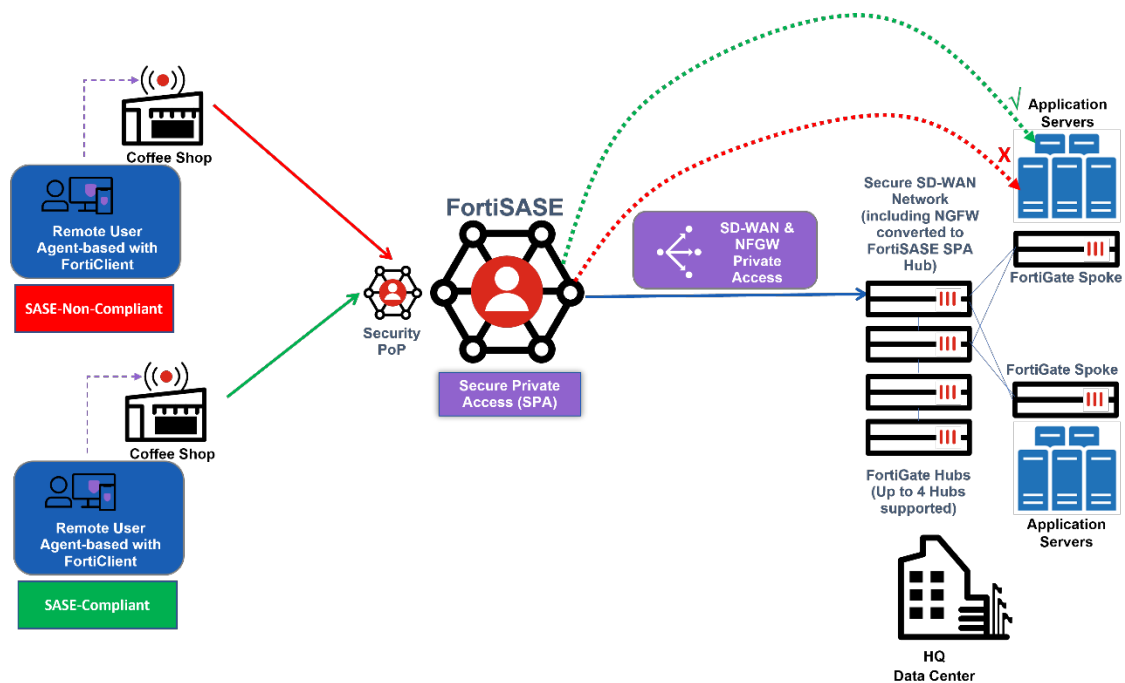
The security settings for Internet and private access are identical. For details on configuring security settings, see [Security on page 92](#).

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 160](#).

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*.

Name

Enabled
☒

Comments

When the following rules match

+ Create

Edit

Delete

☐	Type	Parameters	Matching Criteria
☒	Windows 1		
☐	AntiVirus	AV Software is installed and running	All parameters must pass

Apply the following tag

Tag Name

✖ SASE-Compliant

OK

Cancel

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 62](#) 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 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.

Name ⓘ Allow-SASE-Compliant

Source Scope All VPN Users Thin-Edge

Source All Traffic Specify

✖ SASE-Compliant +

User All VPN Users Specify

Destination Private Access Traffic Specify

4 PrivateServer +

👤 ALL +

Profile Group Default Specify

Force Certificate Inspection ⓘ ☐

Action ☒ Accept ☐ Deny

Status ☒ Enable ☐ Disable

Logging Options

Log Allowed Traffic ☐ Security Events All Sessions

OK Cancel

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, ensure that you order the policies so that the Deny-SASE-Non-Compliant policy is before the Allow-SASE-Compliant policy. With this ordering of policies, FortiSASE denies endpoints that match the dynamic policy from accessing the specific private server.

+ Create Edit Delete Search Internet Access Private Access								
☐	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
☐	Deny-SASE-Non-Compliant		SASE-Non-Compliant	All VPN Users	PrivateServer	Deny	4	Enabled
☐	Allow-SASE-Compliant	Default	SASE-Compliant	All VPN Users	PrivateServer	Accept	11	Enabled
☐	Allow-All Private Traffic	Default	all	All VPN Users	All Private Access Traffic	Accept	0	Enabled
☐	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	Accept	0	Disabled
☐	Implicit Deny		all	All VPN Users	All Private Access Traffic	Deny	14	Enabled

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.



fortinet

- ZERO TRUST TELEMETRY
- REMOTE ACCESS
- ZTNA DESTINATION
- VULNERABILITY SCAN
- Notifications
- Settings
- About



Add Full Name

Phone [Add Phone](#)

Email [Add Email](#)

Get personal info from

- User Input
- OS Updated 1/9/2023 10:21:05 AM
- LinkedIn
- Google
- Salesforce

Status Online/On-fabric

Hostname DESKTOP-BRGB09H

Domain

Zero Trust Tags  SASE-Non-Compliant

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.

+ Create Edit Delete Search Internet Access Private Access								
☐	Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
☐	Deny-SASE-Non-Compliant		🚫 SASE-Non-Compliant	All VPN Users	🖥️ PrivateServer	🚫 Deny	4	🟢 Enabled
☐	Allow-SASE-Compliant	Default	🟢 SASE-Compliant	All VPN Users	🖥️ PrivateServer	🟢 Accept	11	🟢 Enabled
☐	Allow-All Private Traffic	Default	🖥️ all	All VPN Users	All Private Access Traffic	🟢 Accept	0	🟢 Enabled
☐	Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	🟢 Accept	0	🔴 Disabled
☐	Implicit Deny		🚫 all	All VPN Users	All Private Access Traffic	🚫 Deny	14	🟢 Enabled

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:

- 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
```

 - 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/rcv: 1/2
lifetime/rekey: 86400/85206
DPD sent/rcv: 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 users

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

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
```

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:

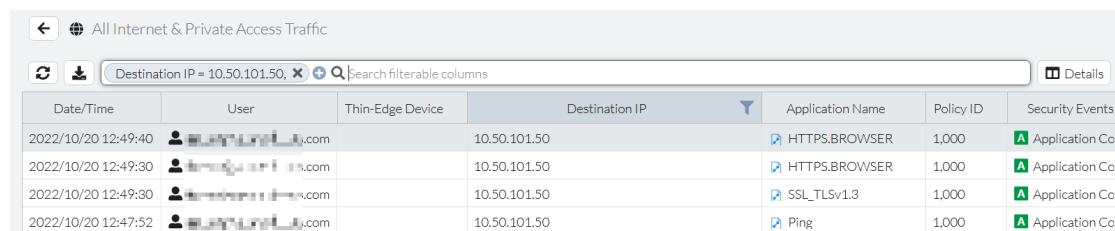
```
get router info bgp summary
get router info bgp neighbors x.x.x.x advertised-routes
```
2. On the GUI, verify routing by going to *Dashboard > Networks*. Click the *Static & Dynamic Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

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.



Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events
2022/10/20 12:49:40	[User Icon] [User Name]		10.50.101.50	HTTPS.BROWSER	1,000	[Green Icon] Application Co
2022/10/20 12:49:30	[User Icon] [User Name]		10.50.101.50	HTTPS.BROWSER	1,000	[Green Icon] Application Co
2022/10/20 12:49:30	[User Icon] [User Name]		10.50.101.50	SSL_TLSv1.3	1,000	[Green Icon] Application Co
2022/10/20 12:47:52	[User Icon] [User Name]		10.50.101.50	Ping	1,000	[Green Icon] Application Co

Following is an example of the *Analytics > Logs > Traffic > Private Access Traffic* page.

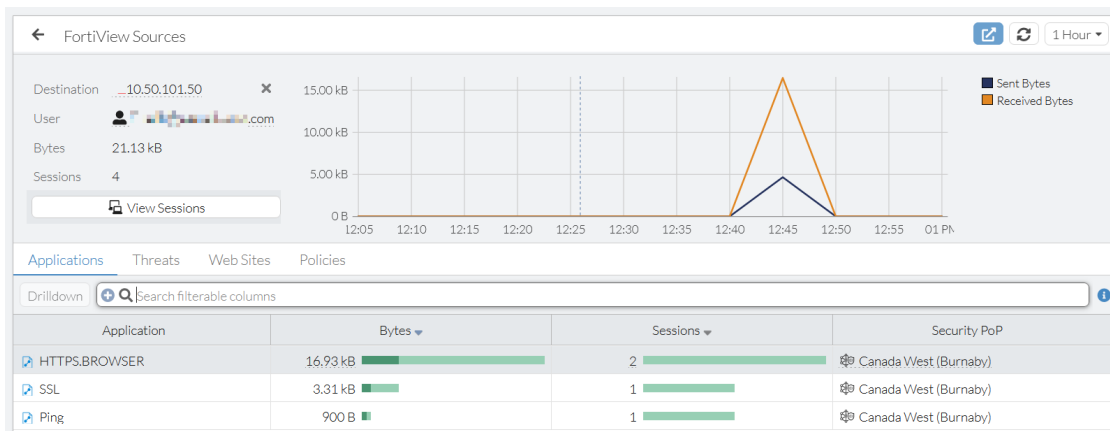
Private Access Traffic

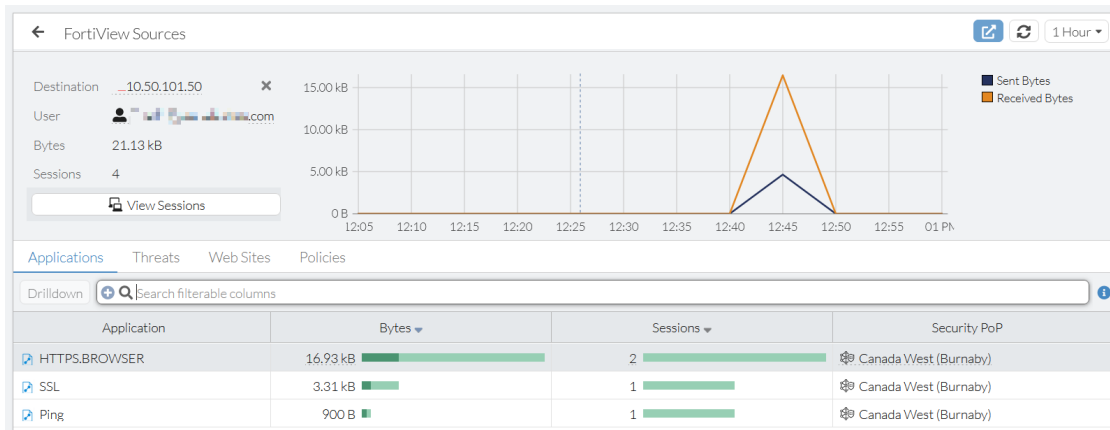
Search filterable columns

Details

Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events	Action
2022/10/20 12:51:02	[User Icon]		10.50.102.50	SSH	1,000	Application Control	Accept: session close
2022/10/20 12:49:40	[User Icon]		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[User Icon]		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[User Icon]		10.50.101.50	SSL.TLSv1.3	1,000	Application Control	Accept: session close
2022/10/20 12:48:04	[User Icon]		10.50.102.50	Ping	1,000	Application Control	Accept
2022/10/20 12:47:52	[User Icon]		10.50.101.50	Ping	1,000	Application Control	Accept
2022/10/20 12:43:33	[User Icon]		192.168.40.150	Ping	1,000	Application Control	Accept
2022/10/20 07:48:21	[User Icon]		10.25.3.4	Ping	1,000	Application Control	Accept
2022/10/20 07:07:51	[User Icon]		10.16.100.1	Ping	1,000	Application Control	Accept
2022/10/20 07:04:29	[User Icon]		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:57	[User Icon]		10.16.101.50	HTTP.BROWSER_Firefox	1,000	Application Control	Accept: session close
2022/10/07 16:38:22	[User Icon]		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:06	[User Icon]		10.16.101.50	Ping	1,000	Application Control	Accept

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.

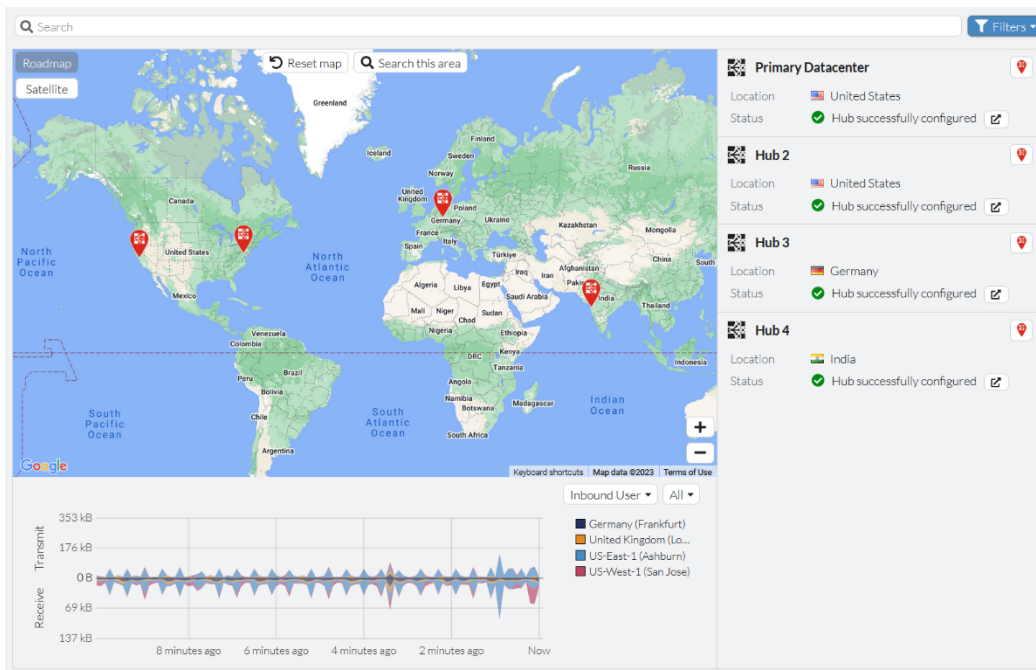




Verifying private access hub status and location using the asset map

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 11](#) 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 14](#) 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

View Endpoint Details Management Connection More Options Search filterable columns Managed Endpoints Unmanaged Endpoints							
Endpoint	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPN	
☒ Windows-User-1	fortinet		Online			Disconnected	Micros
☐ Windows-User-2	fortinet		Online			Disconnected	Micros

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:
 - *View VPN Session*
 - *Show in FortiView*
 - *Show Matching Traffic Logs*
- 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.

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.

View Endpoint Details		Management Connection		More Options		Managed Endpoints		Unmanaged Endpoints	
Search filterable columns									
Endpoint	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPN			
☐ Windows-User-1	fortinet		Online			Disconnected		Micros	

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.

View Endpoint Details		Management Connection		More Options		Managed Endpoints		Unmanaged Endpoints	
Search filterable columns									
Endpoint	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPN			
☒ Windows-User-1	fortinet		Online			Disconnected		Micros	

View Endpoint Details
 Management Connection
 More Options

Enable
 Disable

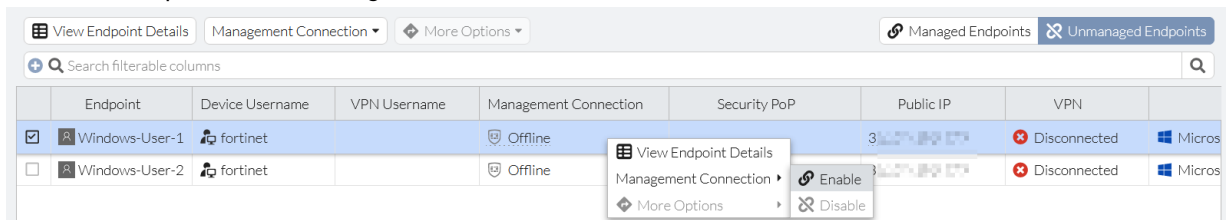
3. Confirm that the endpoint has disappeared from the *Managed Endpoints* view.
4. Go to *Network > Managed Endpoints* and click *Unmanaged Endpoints*. Confirm the endpoint is visible in that view.
5. Go to *Configuration > Users* and click *Onboard Users*.
6. Set *FortiClient Installer* to *Download*.

- Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
- 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.
- 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.

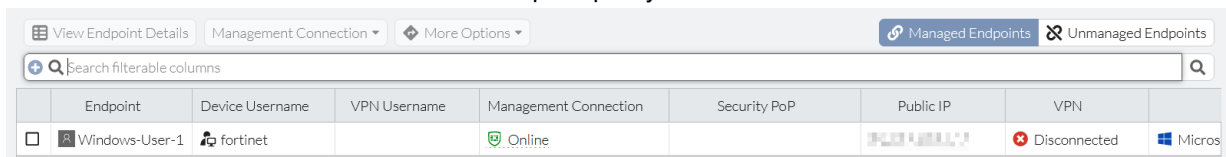
Example: Adding an endpoint to management after it was previously removed

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

- 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.
- Select the endpoint, select *Management Connection > Enable*, and click *OK* to confirm.



- Go to *Configuration > Users* and click *Onboard Users*.
- Set *FortiClient Installer* to *Download*.
- Under *Manual Installer* to the right of the *Invitation Code* field, click the copy icon to copy the invitation code.
- 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.
- 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.



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.

Endpoints **Software Installations**

View Endpoints Search filterable columns

Name	Vendor	Version	First Detected	Last Installed	Endpoint Count
Add Folder Suggestions dialog	Microsoft Corporation	10.0.22000.19	2023/10/05 07:51:38	2021/06/05	1
App Installer	Microsoft Corporation	1.19.10100.1	2023/10/05 07:51:38	2023/04/20	1
Application Verifier x64 External Package	Microsoft	10.1.1904.1	2023/10/05 07:51:38	2022/10/11	1
Assigned Access Lock app	Microsoft Corporation	1000.22000.1	2023/10/05 07:51:38	2021/06/05	1
AsyncTextService	Microsoft Corporation	10.0.22000.1	2023/10/05 07:51:38	2021/06/05	1
Captive Portal Flow	Microsoft Corporation	10.0.21300.1	2023/10/05 07:51:38	2021/06/05	1
CapturePicker	Microsoft Corporation	10.0.19581.1	2023/10/05 07:51:38	2021/06/05	1
ClickOnce Bootstrapper Package for Microsoft .NET ...	Microsoft Corporation	4.8.09000.1	2023/10/05 07:51:38	2022/10/11	1
Cortana	Microsoft Corporation	4.2204.13000.1	2023/10/05 07:51:38	2022/11/01	1
Credential Dialog	Microsoft Corporation	10.0.19591.1	2023/10/05 07:51:38	2021/06/05	1
DiagnosticsHub_CollectionService	Microsoft Corporation	17.3.3000.1	2023/10/05 07:51:38	2022/10/11	1
Email and accounts	Microsoft Corporation	10.0.22000.1	2023/10/05 07:51:38	2021/06/05	1
Eye Control	Microsoft Corporation	10.0.22000.1	2023/10/05 07:51:38	2021/06/05	1
Feedback Hub	Microsoft Corporation	1.2304.10000.1	2023/10/05 07:51:38	2023/05/18	1
FortiClient	Fortinet Technologies Inc	7.0.8.0	2023/10/05 07:51:38	2023/05/18	1
Get Help	Microsoft Corporation	10.2303.10000.1	2023/10/05 07:51:38	2023/05/18	1
Google Chrome	Google LLC	117.0.5938.100	2023/10/05 07:51:38	2023/10/05	1
HEIF Image Extensions	Microsoft Corporation	1.0.61000.1	2023/10/05 07:51:38	2023/05/18	1
icecap_collection_neutral	Microsoft Corporation	17.3.3000.1	2023/10/05 07:51:38	2022/10/11	1

0% 50+

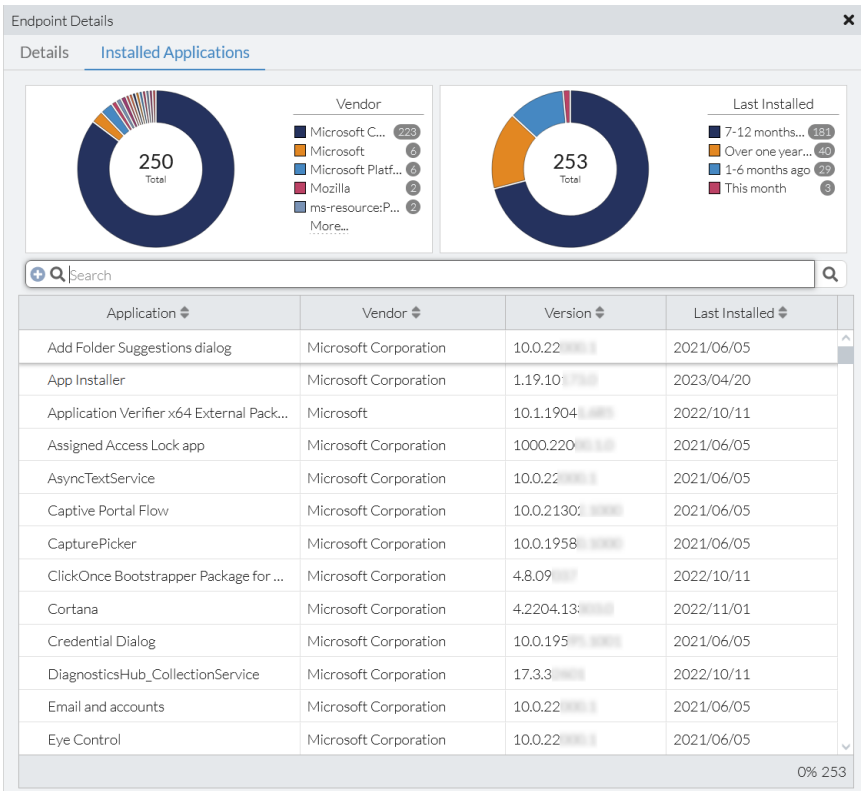
- You can select an application and either click **View Endpoints** or right-click and select **View Endpoints** to view which endpoints have the application installed.

Endpoints with Add Folder Suggestions dialog installed

View Endpoint Details Search

Endpoint	Software OS	Device Username	Last Installed
10.10.10.10	Microsoft Windows 11, 64-bit (build 22000)	Administrator	2021/06/05

- 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*.



The DEM feature requires an Advanced 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.

Digital Experience Monitoring

1 Hour

Drill down

Search

	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.

Digital Experience Monitoring

1 Hour

Drill down		Search						
	SaaS Application	Security PoP	Active Health Events	Jitter (ms)	Start Time	2023/11/08 14:03:59		
					End Time	2023/11/08 15:03:59	MOS	Availability
+	Apple.Services	All Deployed PoPs	Critical: 0 Warning: 0	1.80 (ms)	Average	0.32 (ms)	4.36	100.00%
					Maximum	1.68 (ms)		
					Minimum	0.11 (ms)		
					Standard Deviation	0.33 (ms)		
-	Box	All Deployed PoPs	Critical: 0 Warning: 0	0.22 (ms)			4.40	100.00%

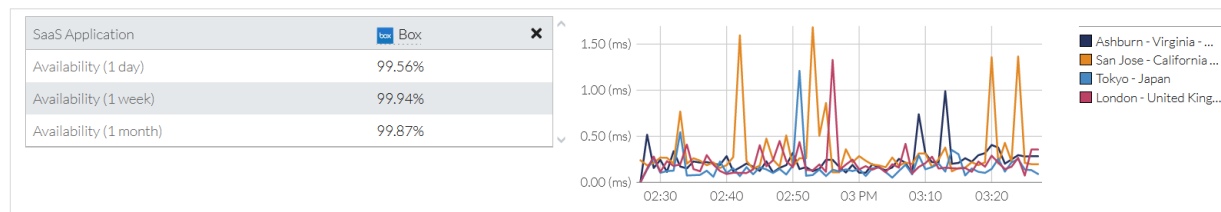
Start Time	2023/11/08 14:03:59
End Time	2023/11/08 15:03:59
Average	0.32 (ms)
Maximum	1.68 (ms)
Minimum	0.11 (ms)
Standard Deviation	0.33 (ms)

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.

Digital Experience Monitoring

 1 Hour ▾


Jitter

Latency

Packet Loss

MOS

Health Events

Q

Search

Time	Ashburn - Virginia - USA	London - United Kingdom	San Jose - California - USA	Tokyo - Japan	Average
2023/11/08 15:27:00	0.28 (ms)	0.36 (ms)	0.20 (ms)	0.09 (ms)	0.23 (ms)
2023/11/08 15:26:00	0.28 (ms)	0.36 (ms)	0.20 (ms)	0.13 (ms)	0.24 (ms)
2023/11/08 15:25:00	0.28 (ms)	0.07 (ms)	0.21 (ms)	0.14 (ms)	0.18 (ms)
2023/11/08 15:24:00	0.29 (ms)	0.27 (ms)	1.37 (ms)	0.25 (ms)	0.54 (ms)
2023/11/08 15:23:00	0.25 (ms)	0.17 (ms)	0.23 (ms)	0.22 (ms)	0.22 (ms)
2023/11/08 15:22:00	0.20 (ms)	0.14 (ms)	0.43 (ms)	0.12 (ms)	0.22 (ms)
2023/11/08 15:21:00	0.38 (ms)	0.21 (ms)	0.20 (ms)	0.25 (ms)	0.26 (ms)
2023/11/08 15:20:00	0.40 (ms)	0.29 (ms)	1.36 (ms)	0.15 (ms)	0.55 (ms)
2023/11/08 15:19:00	0.32 (ms)	0.17 (ms)	0.22 (ms)	0.10 (ms)	0.20 (ms)
2023/11/08 15:18:00	0.29 (ms)	0.22 (ms)	0.19 (ms)	0.11 (ms)	0.20 (ms)
2023/11/08 15:17:00	0.22 (ms)	0.11 (ms)	0.22 (ms)	0.15 (ms)	0.18 (ms)

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

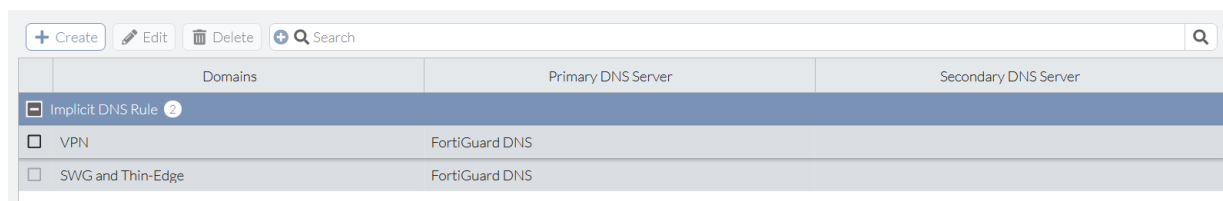
- **Best Fit Columns**
- **Reset Table**
- **Export** displayed data to a file in CSV or JSON format
- **Select Columns**

Configuration

DNS Settings

The *Default DNS Server* setting in FortiSASE 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 82](#).



Domains	Primary DNS Server	Secondary DNS Server
☒ Implicit DNS Rule		
☐ VPN	FortiGuard DNS	
☐ SWG and Thin-Edge	FortiGuard DNS	

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.

You can configure the *Default DNS Server* with one of the following options and 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 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
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 public DNS server other than FortiGuard as follows:

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 default DNS server.

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.

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 115](#) 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 183](#) 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.



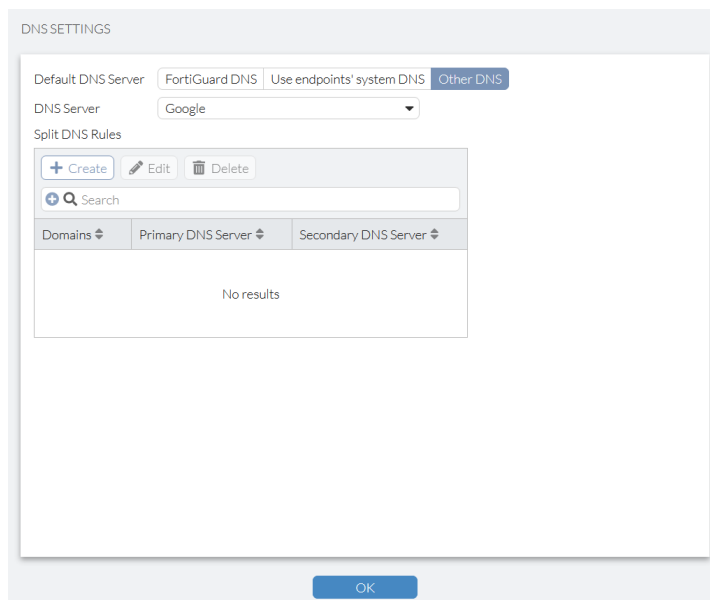
For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE will yield inconsistent results. When an SPA hub is not configured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

Configuring Split DNS Rules

To configure Split DNS Rules:

1. Go to *Configuration > DNS*.
2. Under *Split DNS Rules*, click *Create*.



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



If a *Secondary DNS server* is not available, enter 0.0.0.0 for this field. Currently, this field is mandatory and cannot be skipped.

New Split DNS Rule
✕

Primary DNS Server

Secondary DNS Server

Domains

+

OK
Cancel

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

DNS SETTINGS

Default DNS Server

FortiGuard DNS
Use endpoints' system DNS
Other DNS

DNS Server

Google

Split DNS Rules

+ Create
✎ Edit
🗑 Delete

🔍 Search

Domains	Primary DNS Server	Secondary DNS Server
domain1.com	10.10.10.10	10.10.10.11

OK



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.

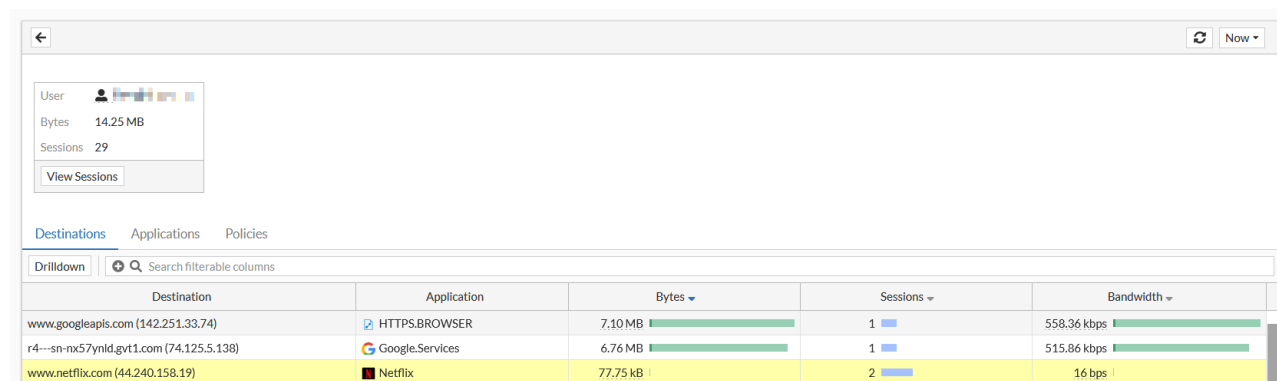
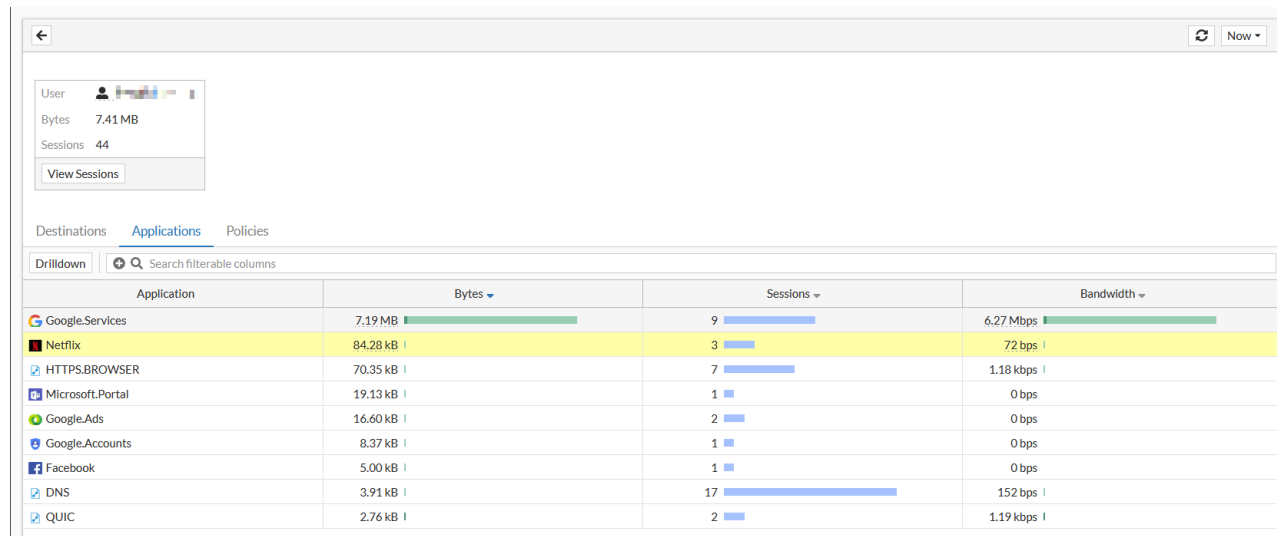
The following provides instructions for configuring the described policies. You may want to configure similar policies, modifying settings based on your environment.

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.

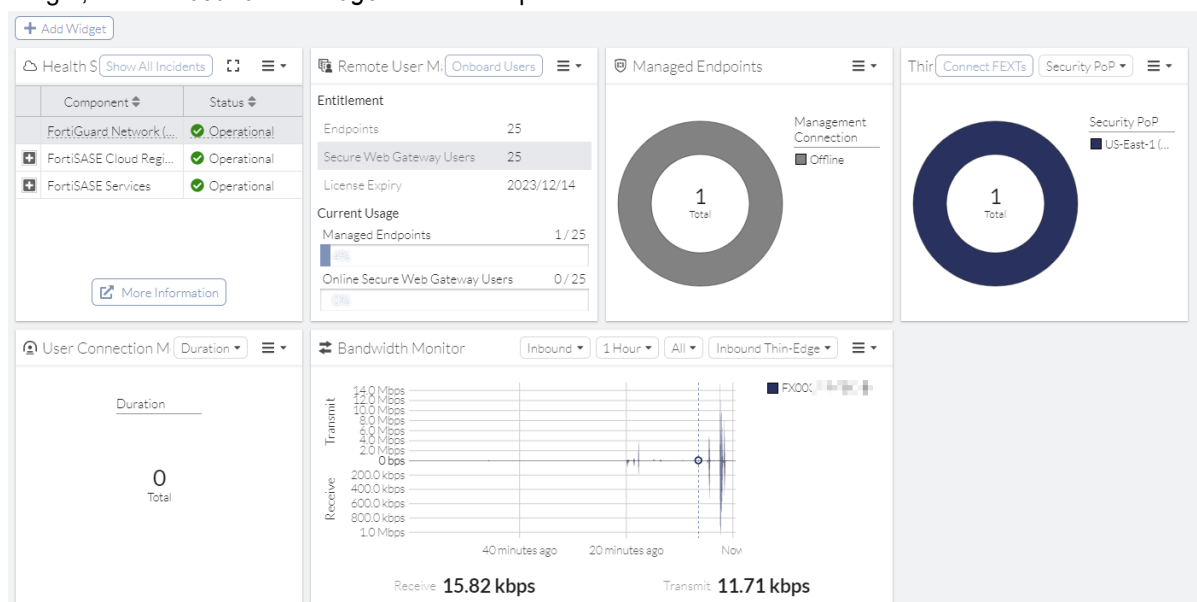


Configuring a policy to allow traffic from the thin-edge LAN to FortiSASE for SIA

To configure a policy to allow traffic from the thin-edge LAN to FortiSASE for SIA:

1. Go to *Configuration > Policies*.
2. Click *Create*.
3. For *Source Scope*, select *Thin-Edge*.
4. In the *Source* field, do one of the following:
 - a. To select all FortiExtenders, select *All Thin-Edge Devices*.
 - b. To specify certain FortiExtenders, select *Specify*, then select the desired FortiExtenders from the *Select Entries* pane.
5. Configure other fields as desired, then click *OK*.
6. You can monitor FortiExtender devices' bandwidth usage by going to *Dashboard > Status*. In the Bandwidth Monitor

widget, select *Inbound Thin-Edge* from the dropdown list.



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 167](#).

Default SWG policies

FortiSASE is configured with the following default 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:

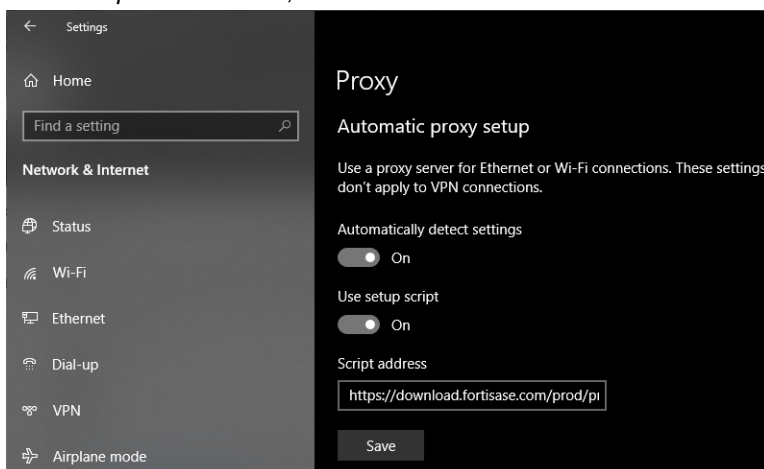
1. Enable SWG configuration:
 - a. Go to *System > SWG Configuration*.
 - b. Toggle *Enable* to on. The GUI may take a few minutes to reload. Once the GUI finishes loading, you can view the *Hosted PAC File* field. Endpoint users use this URL to configure connecting via the FortiSASE SWG server.

- 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 <i>FQDN</i> .

Field	Value
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 115](#).

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 86](#), 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*.
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.

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 115 .

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, there is one global Web Filter configuration that applies to all users.

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. This option also blocks URLs that contains spaces. If there is a space in the URL, it must be written 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.

Option	Description
	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 115 .

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* 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 <code>www.facebook.com</code> in the <i>URL</i> field, it only matches traffic with <code>www.facebook.com</code> . It does not match <code>facebook.com</code> or <code>message.facebook.com</code> . When FortiSASE finds a match, it performs the selected URL action.
Wildcard	Tries to match the pattern based on the rules of wildcards. For example, if you enter <code>*fa*</code> in the <i>URL</i> field, it matches all the content that has <code>fa</code> such as <code>www.facebook.com</code> , <code>message.facebook.com</code> , <code>fast.com</code> , 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 115](#).

To restrict web usage using content filter:

1. Go to *Configuration > Security*.
2. In the *Web Filter* 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.
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 94](#) 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*.
2. In the *Web Filter* widget, click *Customize*.
3. Under *FortiGuard Category Based Filter*, click *Manage Categories*.
4. 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**.

5. Click **OK** again to return to the *Web Filter* pane.
6. Under *Custom Categories*, select the newly created category, then select the desired action. In this example, it is *Block*.
7. 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 115](#).

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](#).

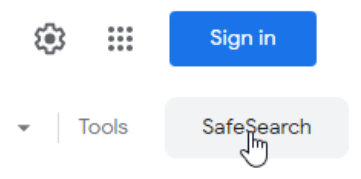
To validate safe search after enforcing it in web filter:



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:



← SafeSearch

Filtering on

SafeSearch helps you manage explicit content in your search results, like sexual activity and graphic violence

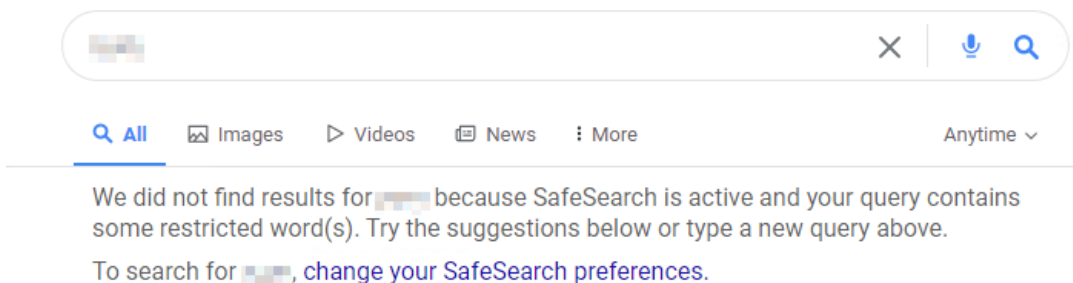
You don't have permission to change your SafeSearch setting. It's locked by safety settings applied to this browser.

More about SafeSearch

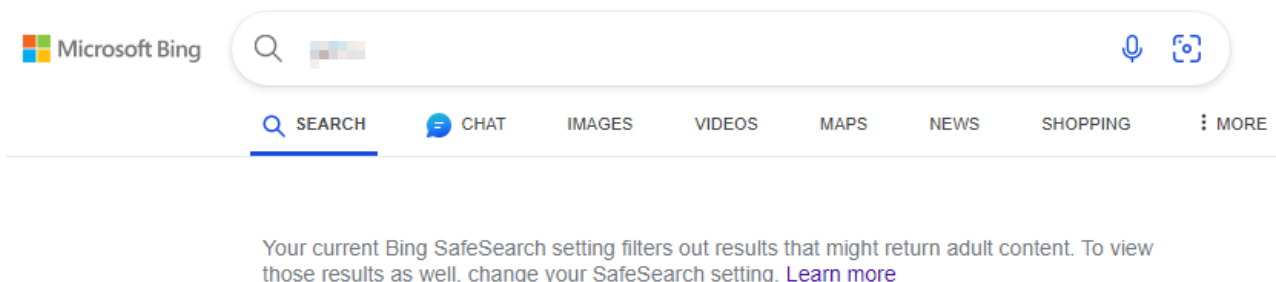


2. Go to a web browser, browse to Yahoo, perform a search, and observe that search results matching safe search criteria are blocked:

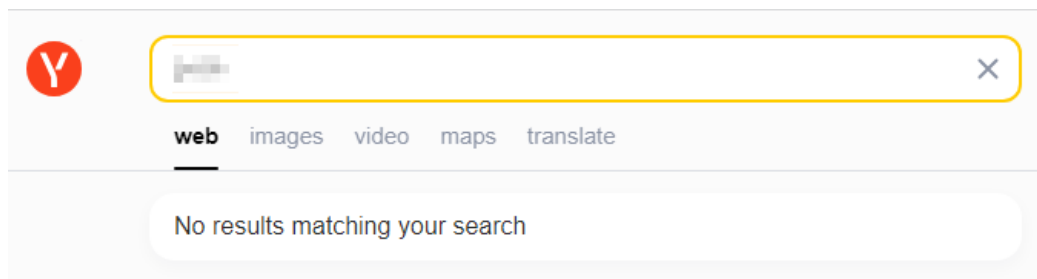
Want more to discover? Make Yahoo Your Home Page. See breaking news & more every time you open your browser.



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

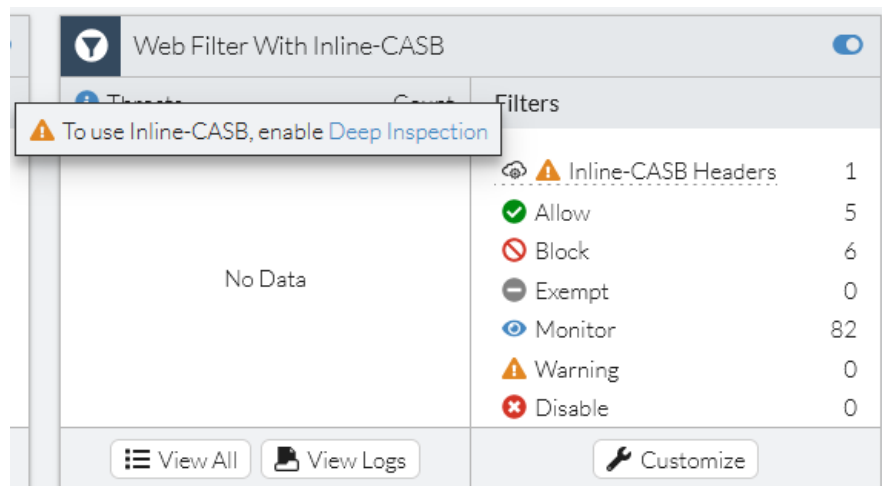
SSL deep inspection

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/remove to header requests/responses, as required by the SaaS application.

- 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 115](#).

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 tenant 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 will only be 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 the SaaS service login page and are only allowed to 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 99](#) 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.

Inline-CASB Header

Header name and content are destination-specific. For more details, please review the documentation. [Documentation](#)

Header name

Header content

Action

Add to request

Destination

+

OK

Cancel

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 92](#).

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 <i>Microsoft Office 365</i> 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	xxxxxxx	Add to request	Create a new address object called wildcard.slack.com containing an FQDN

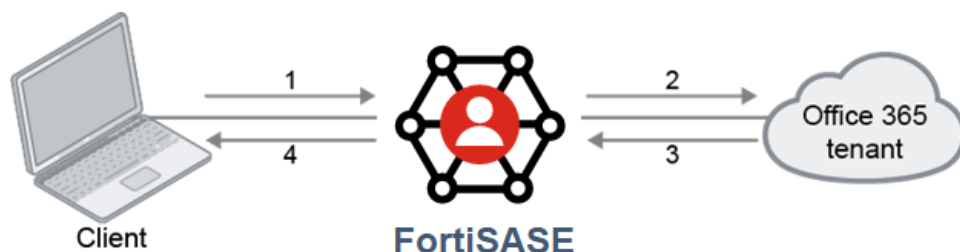
Header name	Header content	Example header content	Action	Destination
	Enterprise Grid account			of *.slack.com
X-Slack-Allowed-Workspaces	Organization IDs or workspace ID	YYYYYY		

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 100](#).

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:

Web Filter With Inline-CASB

Settings
Inline-CASB Headers

+ Create
Edit
Delete
+ Search

Header Name	Header Content	Action	Destination
Restrict-Access-To-Tenants	azure.kldocs.com,kldocs.com,d7cf19c6...	Add to request	Microsoft Office 365
Restrict-Access-Context	d7cf19c6-620c-4e76-9d6e-06e899d...	Add to request	Microsoft Office 365
sec-Restrict-Tenant-Access-Policy	restrict-msa	Add to request	login.live.com

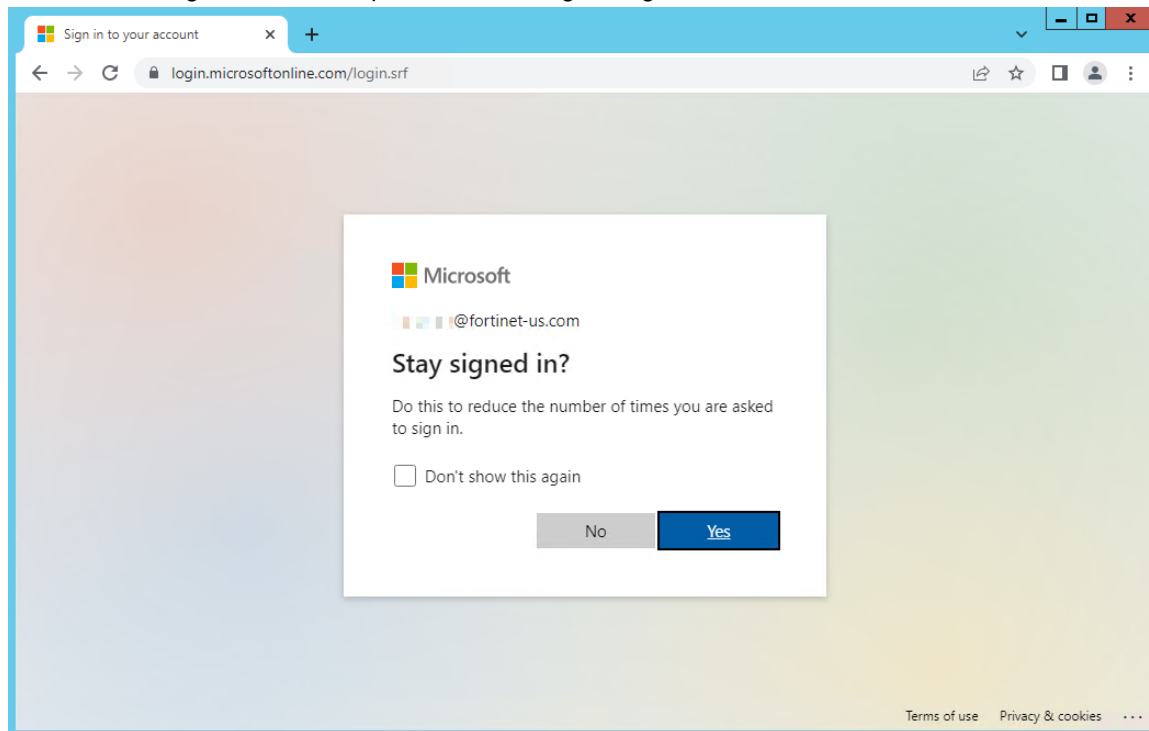
3

OK
Cancel

To test the access to corporate domains and personal accounts:

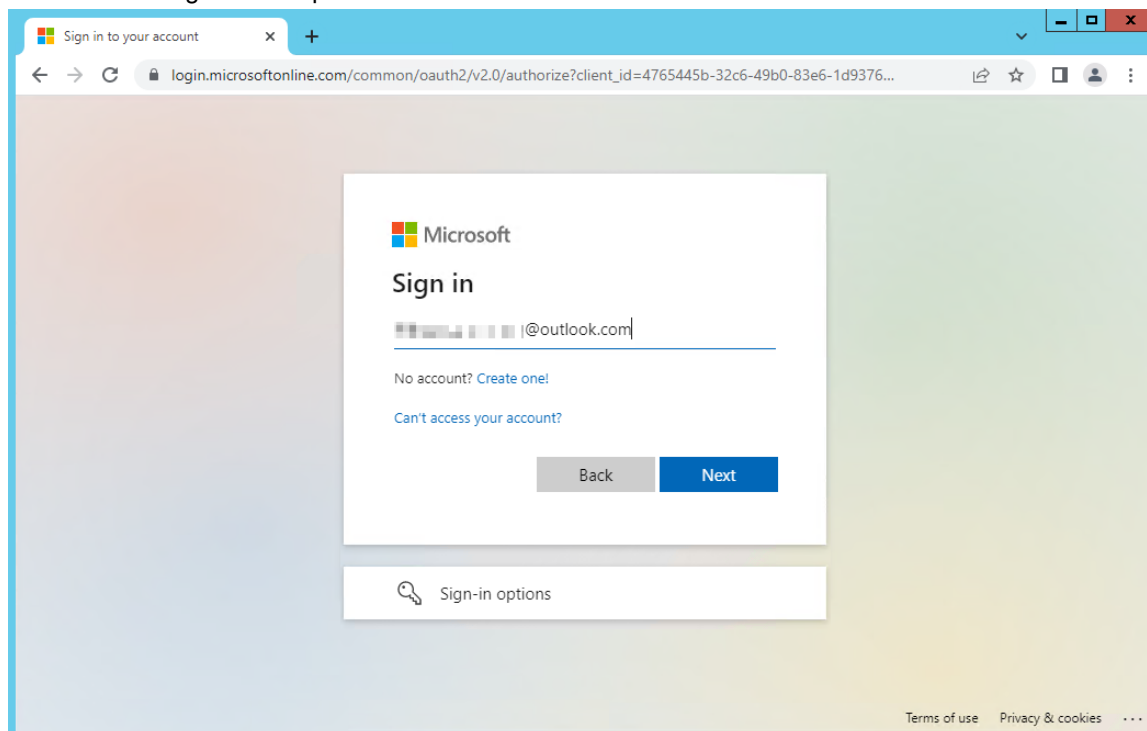
This section outlines the steps for testing the access with a client using a SWG agentless remote user. The steps are similar with a client using a FortiClient agent-based remote user.

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 115 .



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 115](#).

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

FortiSASE 23.4.31 Administration Guide
Fortinet Inc.

111

Enforcing safe search in DNS filter



To enforce safe search, you must use SSL deep inspection. See [Certificate and deep inspection modes on page 115](#).

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 generated by a large number of applications. Application Control With Inline-CASB uses 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).

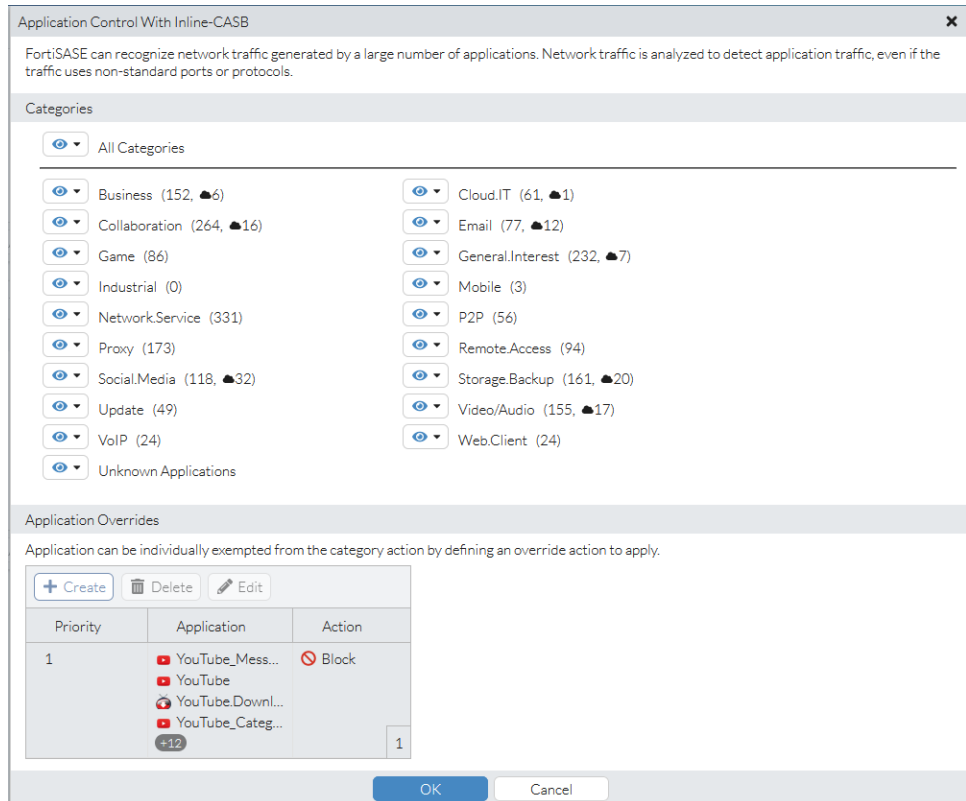
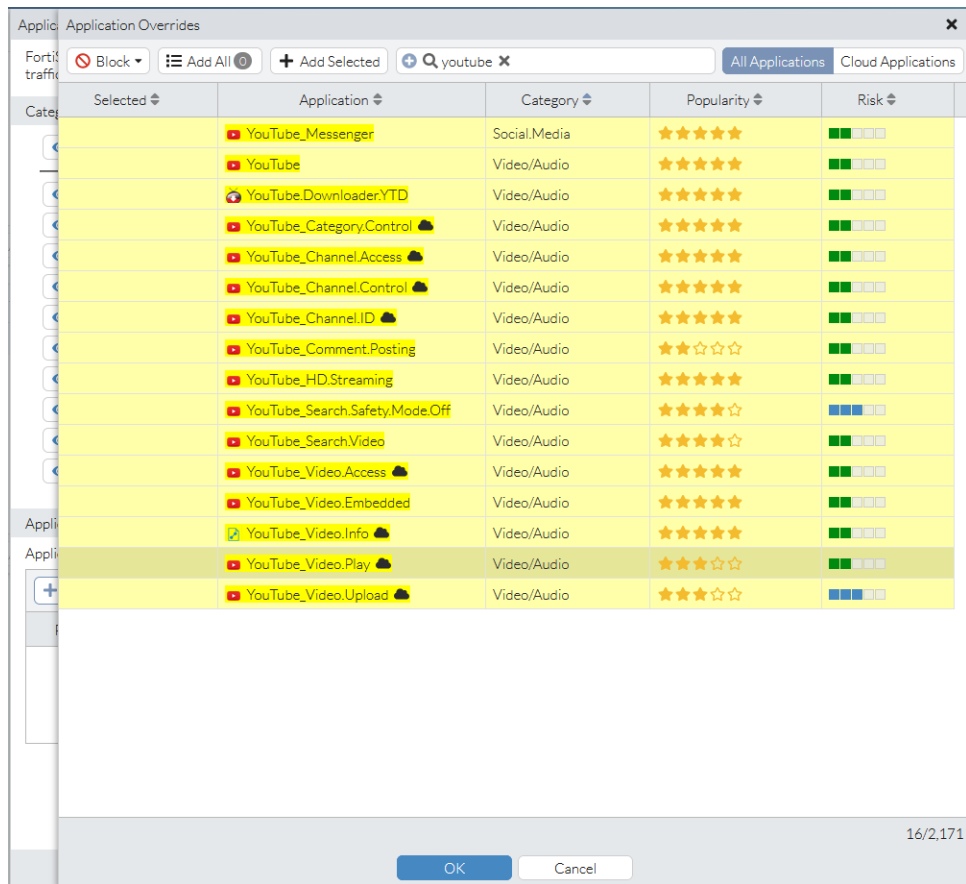
FortiSASE uses Application Control and SSL deep inspection to act as an Inline-cloud access security broker (Inline-CASB) by providing access control to software-as-a-service (SaaS) cloud application traffic. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

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:

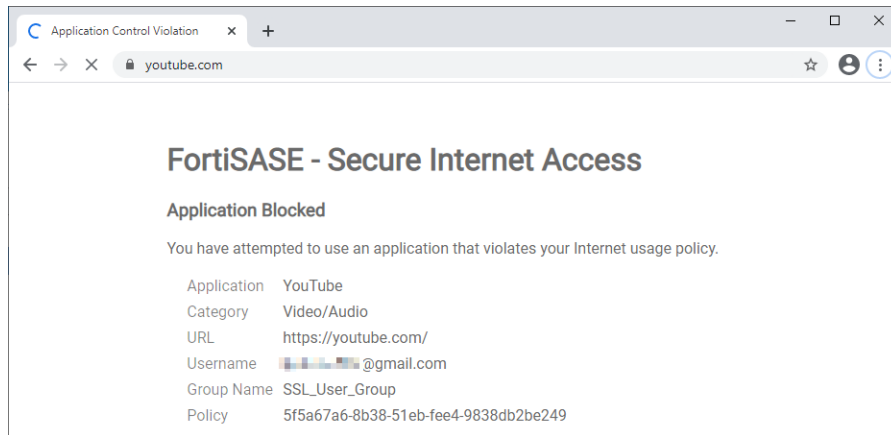
Type	Description
Allow	Passes the traffic to the web filters, antivirus inspection engine, and DLP inspection engine.
Monitor	Processes the traffic the same way as the Allow action. For the Monitor action, FortiSASE generates a log message each time it establishes a matching traffic pattern.
Block	Denies 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*.

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 types of SSL inspection.

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 or deep inspection.

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 certificate inspection is enabled.
Deep inspection	FortiSASE decrypts and inspects the content to find threats and block them. It then re-encrypts 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. SSL inspection can be used 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.

Exempting hosts, URL categories, or service 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. 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 be scanned. 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 the user prevents their connections from SSL deep inspection scanning altogether.

To exempt hosts, URL categories, or services from deep inspection:

1. Go to *Configuration > Security*.
2. In the *SSL Inspection* widget, click *Customize*.
3. Enable *Deep Inspection*.
4. In the *Exempt Hosts*, *URL Categories*, and *Services* fields, click +.
5. In the *Select Entries* pane, select the desired hosts, URL categories, and services 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. In the *SSL Inspection* widget, click *Customize*.
3. Enable *Deep Inspection*.
4. From the *CA Certificate* dropdown list, select *Create*.
5. Configure the fields and upload the certificate and key files as needed.
6. 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 115](#).

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*.

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:

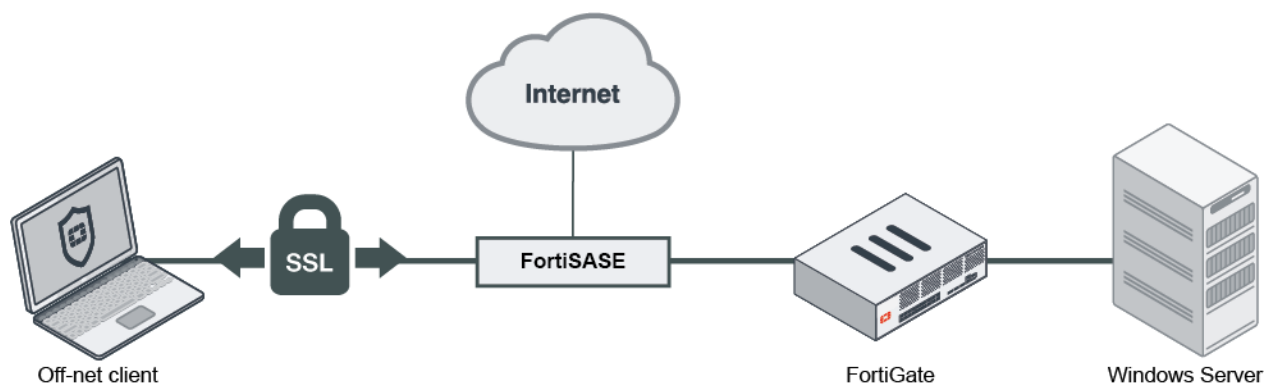
User type	Provisioning process
LDAP	Configure remote users over LDAP to easily integrate FortiSASE with a Windows Active Directory (AD) server or another LDAP server. You can invite users in one of the following ways:

User type	Provisioning process
	- Define an individual user and send the invitation to them directly - Create a user group and send the invitation using the <i>Onboard Users</i> button See Configuring FortiSASE with an LDAP server for remote user authentication in endpoint mode on page 118. See Configuring FortiSASE with an LDAP server for remote user authentication in SWG mode on page 122.
RADIUS	Configure remote authentication with a RADIUS server. You can allow all users from the IdP or define a group in <i>Configuration > Users</i>. Send the invitation code to users using the <i>Onboard Users</i> button. See Configuring FortiSASE with a RADIUS server for remote user authentication on page 125.
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 <i>Configuration > Users</i>. Send the invitation code to users using the <i>Onboard Users</i> button. See: Configuring FortiSASE with Entra ID SSO in endpoint mode on page 127 Configuring FortiSASE with Microsoft Entra ID single sign on in SWG mode on page 131 Configuring FortiSASE with Okta SSO on page 132.
Local	Define user in <i>Configuration > Users</i> and send invitation to them directly. See Users on page 150.

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 endpoint mode

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.

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.
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 <code>cn</code> . Alternatively, you can use <code>sAMAccountName</code> . This is case-sensitive. In other LDAP servers, it may be the user ID, which is denoted <code>uid</code> .
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 <code>dc=KLHOME,dc=local</code> . If you want to look up users under a specific organization unit, specify <code>ou=VPN-Users,dc=KLHOME,dc=local</code> .
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 <i>Certificate</i>, then <i>Create</i>. 2. If you have the certificate file, select <i>File</i>. 3. Click <i>Upload</i>. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in <i>System > Certificates</i> .

Field	Description
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the <i>Server IP/Name</i> 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.
Group Search Base	Enter the search base to use for group searching.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

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 <code>KLHOME\administrator</code> or <code>administrator@KLHOME</code> .
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:
2. To send invitations directly to individual users, do the following:
 - a. Go to *Configuration > Users*.
 - b. Click *Create*.

- c. Select *LDAP User*, then click *Next*.
 - d. From the *LDAP Server* dropdown list, select the server that you configured. Click *Next*.
 - e. FortiSASE displays the available remote users. It displays all users starting from the root of the DN to the subtrees. Select users as desired. Click *Next*.
 - f. Provide the users' email addresses. FortiSASE sends invitation codes and connection instructions to these email addresses.
 - g. Click *OK*.
3. To create and send invitations to a group of users, do the following:
 - a. Create a user group:
 - 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*.
 - viii. Click *OK*.
 - b. Go to *Dashboards > Status*.
 - c. In the *Remote User Management* widget, click *Onboard Users*.
 - d. Under *Invite Users*, enter the email addresses of the users that you want to add to FortiSASE.
 - e. Click *Send*. FortiSASE sends invitation emails to these users so that they can download FortiClient and connect to FortiSASE.

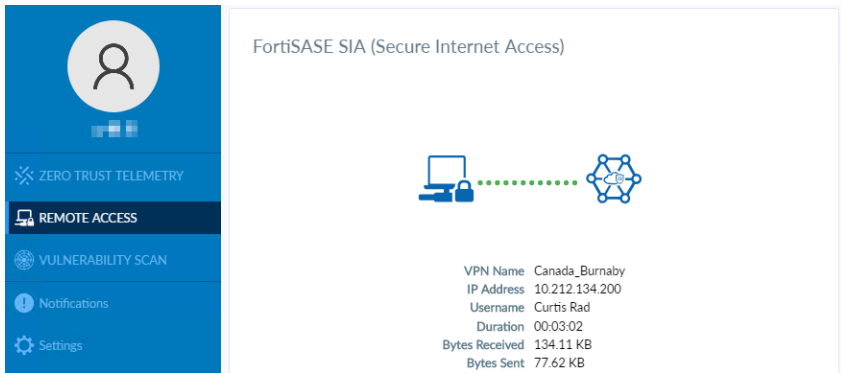
Connecting VPN from FortiClient

The end user follows these instructions to connect to the FortiSASE VPN tunnel.

To connect VPN from FortiClient:

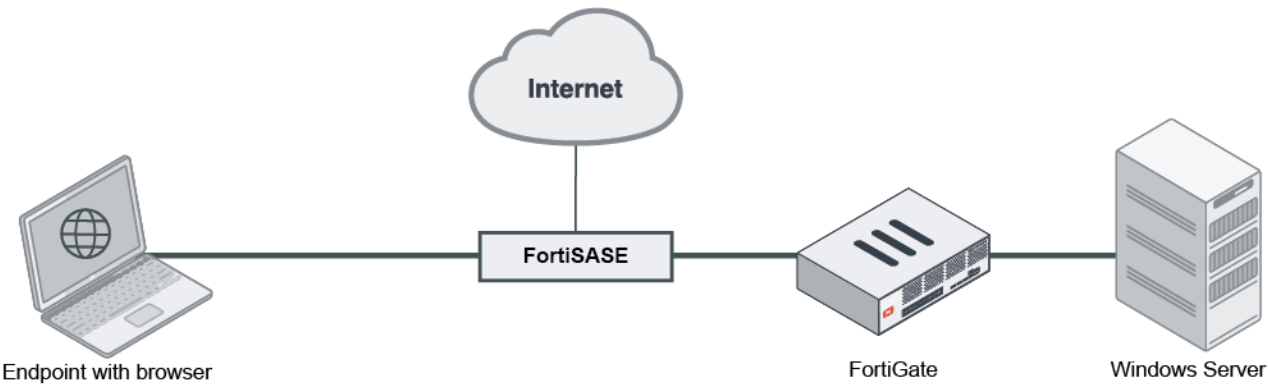
1. Follow the instructions from the received email to install the compatible FortiClient version on to your device.
2. Once installed, open FortiClient.
3. On the *ZERO TRUST TELEMETRY* tab, in the *Join FortiClient Cloud* field, enter the invitation code from the received email.
4. FortiClient connects 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 mode

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 Secure Web Gateway (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.

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.

Field	Description
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 <code>cn</code> . Alternatively, you can use <code>sAMAccountName</code> . This is case-sensitive. In other LDAP servers, it may be the user ID, which is denoted <code>uid</code> .
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 <code>dc=KLHOME,dc=local</code> . If you want to look up users under a specific organization unit, specify <code>ou=VPN-Users,dc=KLHOME,dc=local</code> .
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 <i>Certificate</i>, then <i>Create</i>. 2. If you have the certificate file, select <i>File</i>. 3. Click <i>Upload</i>. This creates a new remote CA certificate in the FortiSASE certificate store. You can also import and view the certificate in <i>System > Certificates</i> .
Server Identity Check	If enabled, the server certificate must include the server IP address/name defined in the <i>Server IP/Name</i> 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.
Group Search Base	Enter the search base to use for group searching.
Member Attribute	Enter the name of the attribute from which FortiSASE retrieves the group membership information.

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 <code>KLHOME\administrator</code> or <code>administrator@KLHOME</code> .
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.

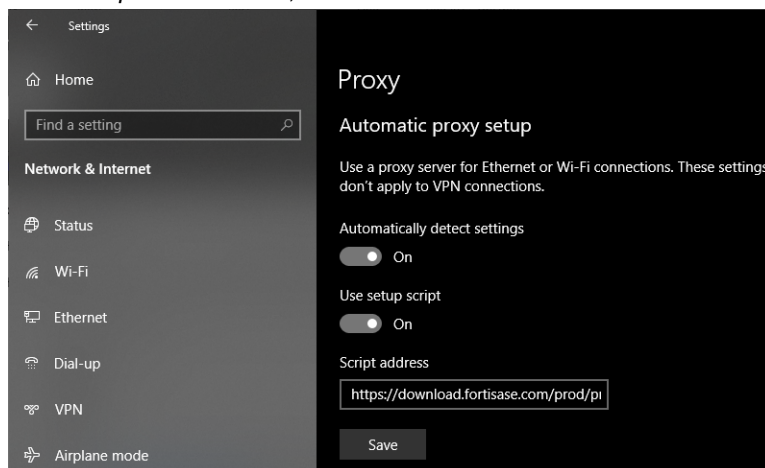
5. Click *Test connection*. If the connection fails, return to the previous steps to reconfigure the LDAP server, or skip the test. If the connection succeeds, click *Next*.
6. Review the configuration, then click *Submit*.

Configuring FortiSASE as an SWG server

The end user follows these instructions to configure SWG 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*.



- 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, as reaching internal RFC 1918 resources from FortiSASE is not supported.

- 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 202](#).
- 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.

To configure the RADIUS server in FortiSASE:

- Go to *Configuration > RADIUS*.
- Click *Create*.
- Configure the following settings:

Field	Description
Name	Connection name.
Authentication Type	If you know the RADIUS server uses a specific authentication protocol, select <i>Specify</i> and select the desired protocol from the list. Otherwise, select <i>Default</i> .
Include All Users	Allow all users on the RADIUS server to authenticate with FortiSASE.

- 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.

- 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*.
- Review the configuration, then click *Submit*.

To invite users using RADIUS authentication to FortiSASE:



The following procedure is not applicable for SWG mode users. See [SWG mode on page 9](#).

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 (formerly known as Azure Active Directory or Azure AD) single sign on (SSO) for endpoint 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

For the *Configure Service Provider* step, this table maps the Entra ID SAML fields that you must copy from FortiSASE and configure in FortiSASE:

FortiSASE SAML field	Entra ID Basic SAML configuration field
IdP Entity ID	Entra ID Identifier

FortiSASE SAML field	Entra ID Basic SAML configuration field
IdP Single Sign-On URL	Login URL
IdP Single Log-Out URL	Logout URL
SAML Claims Mapping > Username	username
SAML Claims Mapping > Group Name	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
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 alphanumeric and less than 30 characters.

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 endpoint mode

You can configure a single sign on (SSO) connection with Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) 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 126](#) 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*.
5. Review the SAML configuration, then click *Submit*.
6. 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.

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 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 (formerly known as Azure Active Directory or Azure AD) 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 SSL 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 an SSL 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 endpoint mode on page 127](#) describes.

- Under *Microsoft Entra ID Options*, click *Configure*.

VPN USER SINGLE SIGN ON (SSO)

☒ Configure Identity Provider
 ☒ Configure Service Provider
 ☒ Review

Service Provider Configuration

Base URL	https://t[redacted].fortisase.com	
Entity ID	https://t[redacted].fortisase.com/remote/saml/	
Assertion Consumer Service (ACS) URL	https://t[redacted].fortisase.com/remote/saml/	
Single Logout Service (SLS) URL	https://t[redacted].fortisase.com/remote/saml/	
Portal (Sign On) URL	https://t[redacted].fortisase.com/remote/login	

Identity Provider Configuration

IdP Entity ID	https://sts.windows.net/d7cf19c6-620c-[redacted]
IdP Single Sign-On URL	https://login.microsoftonline.com/[redacted]/saml2
IdP Single Log-Out URL	https://login.microsoftonline.com/[redacted]/saml2
SAML Claims Mapping	
Username	username
Group Name	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
IdP Certificate	FortiSASE-Test

Azure Active Directory Options

If desired, remote endpoints can be configured to automatically connect to FortiSASE SSL-VPN using Azure AD credentials.
 [Configure](#)

- In the *Microsoft Entra ID Options* slide-in, select *Allow Automatic Sign-on* and enter the domain name and application ID.

Azure Active Directory Options

Allow Automatic Sign-on ☒

Domain Name

Application ID

Instructions for locating the values above on the Azure portal can be found in the documentation.
 [Open Documentation](#)

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

SSL VPN using Entra ID credentials, see the [FortiSASE Agent-based VPN Auto-Connect using Entra ID SSO Deployment Guide](#).

Configuring FortiSASE with Microsoft Entra ID single sign on in SWG mode

You can configure a single sign on (SSO) connection with Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) via SAML, 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 126](#) 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:

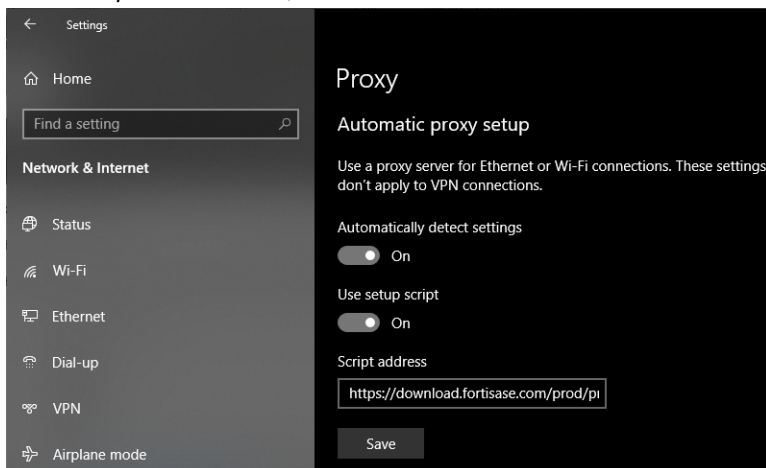
1. In FortiSASE, go to *Configuration > SWG User SSO*. The first step of the SSO configuration wizard displays the entity ID, SSO URL, and single logout URL. You use these values to configure FortiSASE as an SP in Azure. Copy these values.
2. Create and configure your FortiSASE environment in Azure:
 - 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*.
5. Review the SAML configuration, then click *Submit*.

Configuring FortiSASE as a SWG server

The end user follows these instructions to configure SWG 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 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. (Optional) Enable *SAML Claims Mapping*. Only enable this option if you want to use values other than `username` or `group` in the *Username* and *Group Name* fields.
 - c. In the *Username* field, enter `username`. This is case-sensitive.
 - d. In the *Group Name* field, enter `group`. This is case-sensitive.
 - e. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
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 FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO

FortiTrust Identity (FortiTrustID) performs the function of a SAML identity provider (IdP) as well as an IdP proxy and enforces multifactor authentication (MFA). FortiTrustID 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 FortiAuthenticator Cloud as a SAML IdP proxy for Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD).

1. In the Azure portal, do the following:
 - a. Create an enterprise application using FortiSASE as a template from the Azure App Gallery and collect SAML IdP URL information. See [To create an enterprise application using FortiSASE as a template from the gallery: on page 134](#) and [To collect SAML IdP URL information: on page 134](#).
 - b. Find the Entra ID domain and the application ID of the FortiSASE enterprise application. See [To find the Entra ID domain: on page 135](#) and [To find the FortiSASE Azure Enterprise application ID: on page 135](#).
 - c. Register the enterprise application with Microsoft identity platform and generate an authentication key. See [To register the enterprise application: on page 135](#).
 - d. Add the enterprise application as an assignment. See [To add the enterprise application as an assignment: on page 136](#).
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 136](#).
 - b. Create a remote SAML server. See [To configure the remote SAML server: on page 136](#).
 - c. Create a realm for domain name. See [To create an Azure realm and add it to the IdP: on page 137](#).
 - d. Enable SAML IdP portal. See [To enable the SAML IdP portal: on page 138](#).
 - e. Download IdP certificate. See [To download the IdP certificate: on page 138](#).
 - f. Create SAML Service Provider (SP) entry for FortiSASE. See [To create a SAML SP entry for FortiSASE: on page 138](#).
3. In the Azure portal, configure SAML settings for the FortiSASE application in Azure. See [Configuring SAML settings for the FortiSASE application in Azure on page 140](#).
4. In FortiSASE, configure FortiSASE with FortiAuthenticator Cloud in endpoint mode. See [Configuring FortiSASE with FortiAuthenticator Cloud in endpoint mode on page 141](#).

Configuring Azure

Create a new Azure enterprise application using the FortiSASE application as a template from the Azure 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 or endpoint mode deployment.

To create an enterprise application using FortiSASE as a template from the gallery:

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. Assign Entra ID users and groups to FortiSASE.

To collect SAML IdP URL information:

1. Log into the Azure portal.
2. Go to *Microsoft Entra ID > Enterprise applications* and select your newly created application.
3. Go to *Set up single sign on*.
4. For the SSO method, select *SAML*.
5. The *SAML Certificates* box contains links to download the SAML certificate. Download the certificate.
6. The *SAML Certificates* box contains a link to download the Federation Metadata XML. Download the XML file.

7. In the SAML SSO settings for the enterprise application, note these SAML identity provider (IdP) URLs in the *Set up <App Name>* section, which you will use for FortiSASE SAML configuration later:
 - Login URL
 - Entra ID identifier
 - Logout URL

This configure requires that you find the following information from the Azure portal:

- Your Microsoft Entra ID domain
- Your FortiSASE Azure enterprise application ID

The application ID is used to register the FortiClient application to Entra ID and allow it to use the OAuth 2.0 authorization flow. Using this authorization flow, the domain and application ID information along with the currently logged in Windows user's credentials are used by the FortiClient to obtain an access token from Entra ID. As described previously, this access token allows FortiClient to use Entra ID SSO using OAuth 2.0 to establish VPN connections automatically and silently.

To find the Entra ID domain:

1. Log into the Azure portal.
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*.
3. On the *Overview* tab, under *Basic Information*, note the *Primary Domain* listed.

For details on finding the Microsoft Entra ID domain, see [Find the Microsoft Entra ID tenant ID and primary domain name](#).

To find the FortiSASE Azure Enterprise application ID:

1. Log into the Azure portal.
2. On the homepage, do one of the following:
 - Under *Azure Services*, click *Enterprise applications*.
 - Click the navigation menu and under *All Services*, click *Enterprise applications*.
3. On the *All Applications* page, look for the name of your FortiSASE enterprise application and note its application ID. You may need to expand the *Application ID* column to view the complete ID.

For details on finding the an Azure enterprise application ID, see [Quickstart: View enterprise applications](#).

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. Log into the Azure portal.
2. Go to the directory home, and select *Roles and administrators*.
3. From the *Administrative roles* list, select *Directory readers*.
4. Select the ellipsis for *Directory readers*, then select *Description*.
5. Go to *Assignments* and select *Add assignment*.
6. In the *Add assignments* window, search your application by name, and select *Add*.

Configuring FortiAuthenticator Cloud

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 Azure 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 configure the remote SAML server:

1. In FortiAuthenticator Cloud, go to *Remote Auth. Servers > SAML*, and click *Create New*.
2. Select *Proxy* as the *Type*.
3. For the *Entity ID*, click the dropdown menu and select the Azure identity provider (IdP) option.
4. Click *Import IDP metadata/certificate*, and upload the federation metadata file saved previously.
5. For *Send username in this parameter*, enter `login_hint`.
6. Ensure *Strip realm from username before sending* is unchecked.
7. 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.
8. Click *OK* to save changes.

9. Copy the SAML server values:

- a. Select and click *Edit* to edit the recently created Remote SAML server.
- b. Copy the following fields to use when configuring FortiSASE by clicking the copy icon next to each field and pasting it to a file for later use:
 - Portal URL
 - Entity ID
 - ACS (login) URL
 - SLS (logout) URL

You use these fields later when configuring the single sign on settings for the FortiSASE application in Azure.

Edit Remote SAML Server

Name:

Description:

Device FQDN:

Type: ☐ FSO ☒ Proxy

URL Nomenclature: ☒ Individualize ☐ Legacy

Portal URL:

Entity ID:

ACS (login) URL:

IdP Metadata

IdP entity ID:

IdP single sign-on URL:

IdP certificate fingerprints:

Fingerprint algorithm:

Certificate issuer:

Certificate subject:

Validity period:

Authentication context:

Send username in this parameter:

☐ Strip realm from username before sending

☐ Enable IdP-initiated assertion response

☐ Send AuthnRequest with HTTP-POST binding

☐ Sign SAML requests with a local certificate

Single Logout

☒ Enable SAML single logout

SLS (logout) URL:

IdP single logout URL:

Username

Obtain username from: ☐ Subject NameID SAML assertion ☒ Text SAML assertion

Group Membership

Obtain group membership from: ☐ SAML assertions ☐ LDAP lookup ☒ Cloud

OAuth server:

Groups field:

☐ Implicit group membership

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. 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. *Server address*: enter the FortiAuthenticator FQDN.
 - b. *Realms*: 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**.

Certificate ID	Subject	Issuer	Status
31wyg8l.fortitrustrid.forticloud.co	C=AU, ST=New South Wales, L=Sydney, O=Fortin...	C=AU, ST=New South Wal...	Active
Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Call...	Active
Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Call...	Active
Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Call...	Active

To create a SAML SP entry for FortiSASE:

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:
 - a. IdP entity id
 - b. IdP single sign-on URL
 - c. IdP single logout URL
4. Click **Save**.
5. In the *SP Metadata* pane, enter the SP information from FortiSASE, which you will use as the SAML SP:
 - a. SP entity ID
 - b. SP ACS (login) URL
 - c. SP SLS (logout) URL
6. Click **OK**.
7. Select and click *Edit* to edit the recently created SP:
 - a. In *Assertion Attribute Configuration*, configure the following:
 - i. Select *Username* from the *Subject NameID* dropdown list.
 - ii. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.
 - b. In *Assertion Attributes*, select *Add Assertion Attribute* and add the following attributes:
 - i. SAML attribute: *username*
User attribute: SAML username
 - ii. SAML attribute: *groups*
User attribute: SAML group membership
8. Copy the information in step 7b to use for configuring FortiSASE later.

9. Click OK to save changes.

Edit SAML Service Provider

IdP address: 31wygjl.fortitrustid.forticloud.com

SP name: FSS_FACPRICKY_VPN

IdP prefix: kt1iefaat0tewljw

IdP entity id: http://31wygjl.fortitrustid.forticloud.com/saml-idp/kt1iefaat0tewljw/metadata/

IdP single sign-on URL: https://31wygjl.fortitrustid.forticloud.com/saml-idp/kt1iefaat0tewljw/login/

IdP single logout URL: https://31wygjl.fortitrustid.forticloud.com/saml-idp/kt1iefaat0tewljw/logout/

Server certificate: 31wygjl.fortitrustid.forticloud.co | emailAddress=nanz_demo@fortinet.com

IdP signing algorithm: Use default signing algorithms in SAML IDP General page

☐ Support IdP-initiated assertion response

☐ Participate in single logout

SP Metadata

[Import SP metadata](#)

SP entity ID: https://turbo-38vn1axs.edge.stage.fortisase.com/remote/saml/metadata

SP ACS (login) URL: https://turbo-38vn1axs.edge.stage.fortisase.com/remote/saml/login [Alternative ACS URLs](#)

SP SLS (logout) URL: https://turbo-38vn1axs.edge.stage.fortisase.com/remote/saml/logout

☐ SAML request must be signed by SP

Authentication

Authentication method:

- ☐ Mandatory password and OTP
- ☒ All configured password and OTP factors
- ☐ Password-only
- ☐ OTP-only
- ☐ FIDO

Sends username in this parameter: username

Application name for FTM push notification:

☐ Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Subject NameID

Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

☐ Include realm name in subject NameID

Assertion Attributes

Assertion attribute:

SAML attribute: username

User attribute: SAML username

Assertion attribute:

SAML attribute: groups

User attribute: SAML group membership

[Add Assertion Attribute](#)

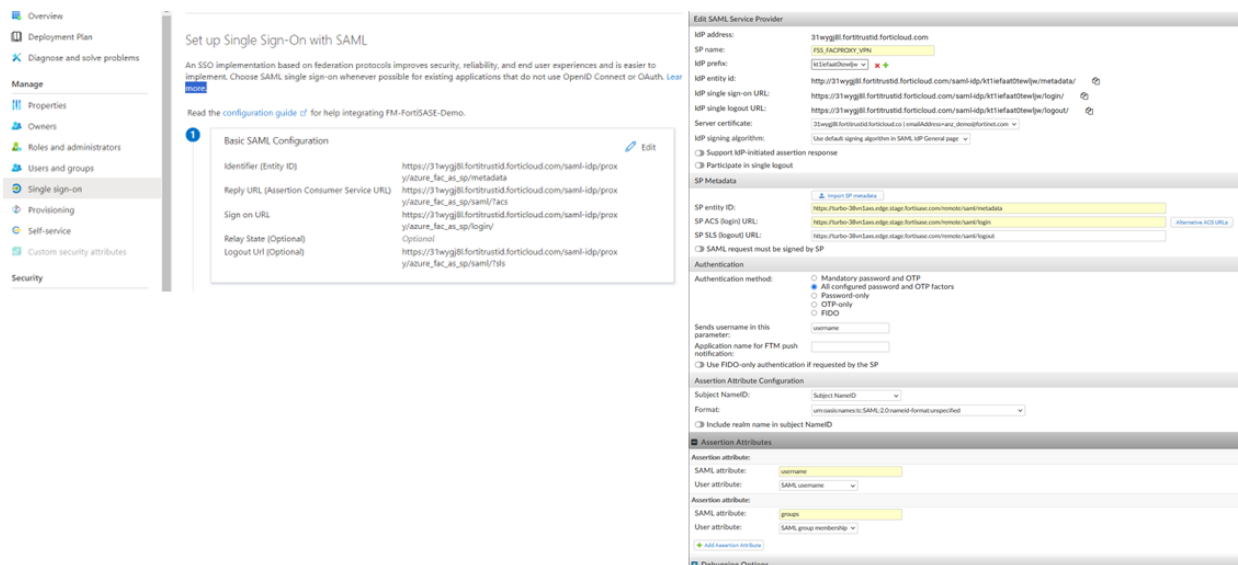
Debugging Options

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 Configuration*, enter the values that you copied in the FortiAuthenticator Cloud Remote SAML Server created in Remote Auth. Servers > SAML in the *Identifier (Entity ID)*, *Reply URL*, *Sign on URL*, and *Logout URL* fields. Click *Save*.

As a reference, the following shows the relation between the Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) IdP and the FortiAuthenticator Cloud Remote SAML Server settings:



Configuring FortiSASE with FortiAuthenticator Cloud in endpoint mode

To configure the FortiAuthenticator Cloud IdP information in FortiSASE:

1. In FortiSASE, go to *Configuration > VPN User SSO* and click *Next* in the single sign on (SSO) wizard.
2. In the *IdP Entity ID*, *IdP Single Sign-On URL*, and *IdP Single Log-Out URL* fields, paste the values that you copied from the FortiAuthenticator Cloud SAML IdP > *Service Providers* fields.
3. From the *IdP Certificate* dropdown list, select *Create*, then upload the certificate that you downloaded. Click *Next*.
4. Review the SAML configuration, then click *Submit*.
5. 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.

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 endpoint mode via *Configuration > VPN User SSO*, or in SWG mode via *Configuration > SWG User SSO*.

Determining Entra ID SSO credentials

Before you can search user groups from Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) single sign on (SSO), you must perform some preliminary steps and then determine the SAML provider credentials from the Entra ID portal.

To access the Entra ID portal:

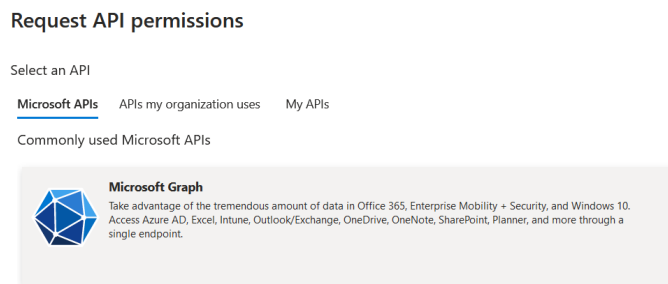
1. Log into the Azure portal. You should already have an enterprise application created in Entra ID. If this has not been created, see [Creating an enterprise application using FortiSASE as a template from the gallery and collecting SAML IdP URL information](#).
2. On the homepage, do one of the following:
 - 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 searching user groups:

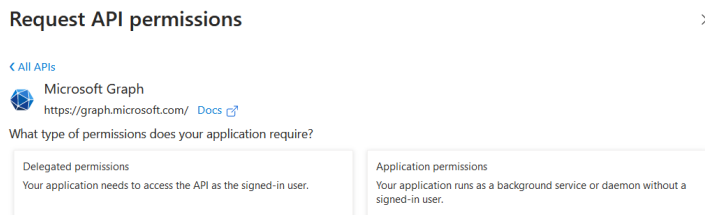
1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE SSL VPN enterprise application and click the hyperlinked name.
3. In the left menu, click *API permissions*, and click *Add a permission*.

The screenshot shows the Microsoft Entra ID portal interface. The breadcrumb navigation at the top reads: Home > Default Directory | App registrations > FM-FortiSASE-Test. The main header of the page is "FM-FortiSASE-Test | API permissions". On the left, there is a navigation menu with sections: "Overview" (with sub-items: Overview, Quickstart, Integration assistant) and "Manage" (with sub-items: Branding & properties, Authentication, Certificates & secrets, Token configuration, and API permissions, which is currently selected). The main content area has a search bar, "Refresh", and "Got feedback?" links. Below these are two informational messages: a yellow warning about user consent and a blue information message about the "Admin consent required" column. The "Configured permissions" section states that applications are authorized to call APIs when granted permissions by users/admins. At the bottom, there is a link to "Add a permission" and a checked checkbox for "Grant admin consent for Default Directory".

4. In the *Request API permissions* slide-in window, click *Microsoft Graph*.



5. Select *Application permissions*.



6. In the *Select permissions* section, search for, and select the following permissions by clicking the checkboxes next to these permissions:
- Group.Read.All – Read all groups
 - GroupMember.Read.All – Read all group memberships
7. Click *Add permissions*.
8. In the *API permissions* page, click *Grant admin consent for Default Directory*. If this option is grayed out, you must log into an Entra ID admin account to perform this step.

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 SSL VPN 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 window, 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 *Azure Client Secret*. This value is not visible after this initial

creation step and moving to another page.

[Home](#) > [Default Directory | App registrations](#) > [FM-FortiSASE-Test](#)

FM-FortiSASE-Test | Certificates & secrets

Description	Expires	Value	Secret ID
20230517	11/13/2023	q2E8Q...	cc86de...

To determine the tenant and client IDs:

1. In the left menu, click *App registrations*, then click the *All applications* tab.
2. Look for the name of your FortiSASE SSL VPN enterprise application 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 *Azure Client ID*
 - *Directory (tenant) ID*, which FortiSASE uses as the *Azure Tenant ID*

Therefore, in summary, you should note the following credentials:

Entra ID page within specific enterprise application	Entra ID field	FortiSASE field
Overview	Directory (tenant) ID	Azure Tenant ID
Overview	Application (client) ID	Azure Client ID
Certificates & Secrets	Value	Azure 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 an endpoint 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 endpoint 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 the *SAML Remote User Groups* dropdown list next to and notice that the groups are dynamically obtained from Entra ID and populated. Select a remote user group from the populated dropdown list and click *OK* to save the changes.
7. Notice that the *Configure Service Provider* page has the *Group ID* automatically filled in with the selected user group's Azure group object ID. 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.



Currently, testing SSO configuration from FortiSASE is supported for endpoint mode using either 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 endpoint mode on page 127](#).

2. In right-hand gutter, click *Start Test*.

VPN USER SINGLE SIGN ON (SSO)

Configure Identity Provider Configure Service Provider Review

Service Provider Configuration

Base URL:

Entity ID:

Assertion Consumer Service (ACS) URL:

Single Logout Service (SLS) URL:

Portal (Sign On) URL:

User Groups

Create a [User Group](#) in FortiSASE to map to any user group that exists on your remote authentication source. User Groups can be used within Policies to explicitly allow or deny traffic for subsets of users.

[@ Onboard Users](#)

Test SSO Configuration

SSO configuration can be tested end-to-end by logging into a user account configured on your SSO server. The test will time out if FortiSASE does not get a successful log-in response from your IdP within a minute. Navigating to another page will cancel the test.

[Start Test](#)

Useful Links



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.

SSO Configuration Test Output

Test Results Raw Log Output

1. Start SSO Configuration Test ✓

FortiSASE reads your SSO configuration and prepares the browser for redirection to the Identity Provider sign on page. If errors occur here review your SSO configuration to ensure it is compatible with your Identity Provider.

IdP Single Sign-On URL: <https://login.microsoftonline.com/...>

2. FortiSASE to IdP SAML Authentication Request ✓

FortiSASE has redirected the browser to the Identity Provider sign on page. If errors occur here ensure network connectivity to your Identity Provider is stable and your SSO configuration is correct.

```

1 <lasso:Login
2   xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
3   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
4   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
5   LoginDumpVersion="2"
6 ><lasso:Request
7   ><samlp:AuthnRequest
8     ID="_7DAABF3C9A0EE3119E7F6EEE9F4D7D25"
9     Version="2.0"
10    IssueInstant="2023-05-17T06:14:12Z"
11    Destination="https://login.microsoftonline.com/..."
12    SignType="0"
13    SignMethod="0"
14    ForceAuthn="false"
15    IsPassive="false"
16    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
17    AssertionConsumerServiceURL="https://...fortisase.com/remote/saml/login"

```

3. IdP to FortiSASE SAML Authentication Response ✓

FortiSASE has received the SAML assertion from your Identity Provider. The assertion is processed and authorization finalizes. If errors occur here there may be issues with your SSO configuration. Here are some debugging tips:

1. Review the raw log output for any potential failure cases.
2. Ensure that the SSO configuration matches what your Identity Provider expects.

Username:

Group:

Close Download Raw Logs

The following shows an example *Test Results* tab with a failed test step that an identity provider entity ID misconfiguration caused.

SSO Configuration Test Output

Test Results Raw Log Output 1

SSO configuration test timed out. ✕

2. FortiSASE to IdP SAML Authentication Request ✓

FortiSASE has redirected the browser to the Identity Provider sign on page. If errors occur here ensure network connectivity to your Identity Provider is stable and your SSO configuration is correct.

```

1 <lasso:Login
2   xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
3   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
4   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
5   LoginDumpVersion="2"
6   ><lasso:Request
7     ><samlp:AuthnRequest
8       ID="_7CB2531E8F32E60F60A548A36D5AA677"
9       Version="2.0"
10      IssueInstant="2023-05-17T07:44:59Z"
11      Destination="https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2"
12      SignType="0"
13      SignMethod="0"
14      ForceAuthn="false"
15      IsPassive="false"
16      ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
17      AssertionConsumerServiceURL="https://turbo-s691kc8a.edge.stage.fortisase.com/remote/saml/login"

```

3. IdP to FortiSASE SAML Authentication Response ✕

FortiSASE has received the SAML assertion from your Identity Provider. The assertion is processed and authorization finalizes. If errors occur here there may be issues with your SSO configuration. Here are some debugging tips:

1. Review the raw log output for any potential failure cases.
2. Ensure that the SSO configuration matches what your Identity Provider expects.

Username:

Group:

```

1 <samlp:Response
2   ID="_9c71e586-bf3b-419a-9700-96094a09f6d3"
3   Version="2.0"
4   IssueInstant="2023-05-17T07:45:05.825Z"
5   Destination="https://turbo-s691kc8a.edge.stage.fortisase.com/remote/saml/login"
6   InResponseTo="_7CB2531E8F32E60F60A548A36D5AA677"
7   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

```

Close Download Raw Logs

- 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.

SSO Configuration Test Output

Test Results

Raw Log Output

```

* SAML_INFO: Found server 'FORTISASE_SAML_SERVER' in group 'VPN_SSO_AUTH_GROUP'
* SAML_BROWSER_START_TEST: Processing login request
* SAML_EVENT: Creating login request redirect form
* SAML_EVENT: Generated redirection url: https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2?SAMLRequest=pZJBb9sgFMe%2FisUd2zipXaMkKhs7WqRus5p0h10mip9TNAwZD3fbty%2Bxt647rJddkHi8P%2FD76a1QDPmQ9E%2Fmjv4NgL%2B%2FFwJFH1W9LWGHwHcAdwT0rC%2Fd3tHyA%2FugdLMS%2FZV3ktYuhOEActYe1tCKPAGc%2FBYD1MALMEs1ldNnxS6Tb%2Fc98AXnTCi1Xy%2BsbVPF%3D%3D&RelayState=magic%3D9af218ad69f4a92d&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=YA20YwPHI%2BzTi%2BFz5mRttg7cxVewZuQI%2FWuZ8LiKIDcquHe2a8%2B3iJdwwF6TkOU5RSWiZVfWUCpnSiTw4%2BwkZIXu3yc3j9iLsd%3D%3D
* SAML_SP_REDIRECTED_BROWSER_TO_IDP: Redirecting browser
* SP_REQUEST_XML: <lasso:Login xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest ID="_7DAABF3C9A0EE3119E7F6EEE9F4D7D25" Version="2.0" IssueInstant="2023-05-17T06:14:12Z" Destination="https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2" SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="https://turbo-s691kc8a.edge.stage.fortisase.com/remote/saml/login"><saml:Issuer>https://turbo-s691kc8a.edge.stage.fortisase.com/remote/saml/metadata</saml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProviderID>https://sts.windows.net/d7cf19c6-620c-4e76-9d6e-06e899de34f2/</lasso:RemoteProviderID><lasso:MsgUrl>https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2?SAMLRequest=pZJBb9sgFMe%2FisUd2zipXaMkKhs7WqRus5p0h10mip9TNAwZD3fbty%2Bxt647rJddkHi8P%2FD76a1QDPmQ9E%2Fmjv4NgL%2B%2FFwJFH1W9LWGHwHcAdwT0rC%2Fd3tHyA%2FugdLMS%2FZV3ktYuhOEActYe1tCKPAGc%2FBYD1MALMEs1ldNnxS6Tb%2Fc98AXnTCi1Xy%2BsbVPF%3D%3D&RelayState=magic%3D9af218ad69f4a92d&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=YA20YwPHI%2BzTi%2BFz5mRttg7cxVewZuQI%2FWuZ8LiKIDcquHe2a8%2B3iJdwwF6TkOU5RSWiZVfWUCpnSiTw4%2BwkZIXu3yc3j9iLsd%3D%3D/</lasso:MsgUrl><lasso:MsgRelayState>magic=9af218ad69f4a92d</lasso:MsgRelayState><lasso:HttpRequestMethod>4</lasso:HttpRequestMethod><lasso:RequestID>_7DAABF3C9A0EE3119E7F6EEE9F4D7D25</lasso:RequestID></lasso:Login>
* SAML_IDP_REDIRECTED_BROWSER_TO_SP: Redirected from IdP
* IDP_RESPONSE_XML: PHNhbwXwO1Jlc3Bvb3N1IElEPSjFMDNhZTI2ZTMtNGQ4ZS00N2NmLTk4N2ctM2V1MDg0ZWZiZWVmIiBwZXJzaW9uPSIyLjAiIElzc3V1SW5zdGFudD0iMj,
* SAML_PROCESS_LOGIN_RESPONSE: Processing login response
* SAML_RESPONSE_GROUP: 'https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2?SAMLRequest=pZJBb9sgFMe%2FisUd2zipXaMkKhs7WqRus5p0h10mip9TNAwZD3fbty%2Bxt647rJddkHi8P%2FD76a1QDPmQ9E%2Fmjv4NgL%2B%2FFwJFH1W9LWGHwHcAdwT0rC%2Fd3tHyA%2FugdLMS%2FZV3ktYuhOEActYe1tCKPAGc%2FBYD1MALMEs1ldNnxS6Tb%2Fc98AXnTCi1Xy%2BsbVPF%3D%3D&RelayState=magic%3D9af218ad69f4a92d&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=YA20YwPHI%2BzTi%2BFz5mRttg7cxVewZuQI%2FWuZ8LiKIDcquHe2a8%2B3iJdwwF6TkOU5RSWiZVfWUCpnSiTw4%2BwkZIXu3yc3j9iLsd%3D%3D'
* SAML_RESPONSE_USER: 'https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2/saml2?SAMLRequest=pZJBb9sgFMe%2FisUd2zipXaMkKhs7WqRus5p0h10mip9TNAwZD3fbty%2Bxt647rJddkHi8P%2FD76a1QDPmQ9E%2Fmjv4NgL%2B%2FFwJFH1W9LWGHwHcAdwT0rC%2Fd3tHyA%2FugdLMS%2FZV3ktYuhOEActYe1tCKPAGc%2FBYD1MALMEs1ldNnxS6Tb%2Fc98AXnTCi1Xy%2BsbVPF%3D%3D&RelayState=magic%3D9af218ad69f4a92d&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=YA20YwPHI%2BzTi%2BFz5mRttg7cxVewZuQI%2FWuZ8LiKIDcquHe2a8%2B3iJdwwF6TkOU5RSWiZVfWUCpnSiTw4%2BwkZIXu3yc3j9iLsd%3D%3D'
* SAML_WARN: Found a group with no match setting: 'VPN_SSO_AUTH_GROUP'
* SAML_WARN: Requires client cert: 0
* SAML_INFO: Adding SAML group info

```

Close

Download Raw Logs

The following shows an example *Raw Log Output* tab with a failed test step that an identity provider entity ID misconfiguration caused.

```
SSO Configuration Test Output

Test Results Raw Log Output 1

* SAML_INFO: Found server 'FORTISASE_SAML_SERVER' in group 'VPN_SSO_AUTH_GROUP'
* SAML_BROWSER_START_TEST: Processing login request
* SAML_EVENT: Creating login request redirect form
* SAML_EVENT: Generated redirection url: https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2
/saml2?SAMLRequest=pZjdb9sgF1b%2FisW9v20coySSmzRapG6zmmwXvZkoPk7RDGQc3G3%2FvsRut%2B5ivekNEofzAs%2Bjs0SuhjNrRvegb%2BHHCoi%
%2F%2B07voJ&RelayState=magic%3D85270efcd7ef1f79&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&
Signature=Z0WZtCSwhaIFmg5My25HCgYnX9ZZ%2FeyJJWl1eqZj7Wjhji%2B04ctoPFbx4K4ilMnj%2FHCYRHZ1MIS10%2F0V98M1nmpHHLGbcImm2pjay0
%3D%3D
* SAML_SP_REDIRECTED_BROWSER_TO_IDP: Redirecting browser
* SP_REQUEST_XML: <lasso:Login xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest ID="_7CB2531E8F32E60F60A548A36D5AA677" Version="2.0"
IssueInstant="2023-05-17T07:44:59Z" Destination="https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-06e899de34f2
/saml2" SignType="0" SignatureMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="https://turbo-
s691kc8a.edge.stage.fortisase.com/remote/saml/login"><saml:Issuer>https://turbo-s691kc8a.edge.stage.fortisase.com
/remote/saml/metadata</saml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProviderID>https://sts.windows.net/d7cf19c6-620c-
4e76-9d6e-06e899de34f2/</lasso:RemoteProviderID><lasso:MsgUrl>https://login.microsoftonline.com/d7cf19c6-620c-4e76-9d6e-
06e899de34f2
/saml2?SAMLRequest=pZjdb9sgF1b%2FisW9v20coySSmzRapG6zmmwXvZkoPk7RDGQc3G3%2FvsRut%2B5ivekNEofzAs%2Bjs0SuhjNrRvegb%2BHHCoi%
%2F%2B07voJ&RelayState=magic%3D85270efcd7ef1f79&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&
Signature=Z0WZtCSwhaIFmg5My25HCgYnX9ZZ%2FeyJJWl1eqZj7Wjhji%2B04ctoPFbx4K4ilMnj%2FHCYRHZ1MIS10%2F0V98M1nmpHHLGbcImm2pjay0
%3D%3D</lasso:MsgUrl><lasso:MsgRelayState>magic=85270efcd7ef1f79</lasso:MsgRelayState>
<lasso:HttpRequestMethod>4</lasso:HttpRequestMethod>
<lasso:RequestID>_7CB2531E8F32E60F60A548A36D5AA677</lasso:RequestID></lasso:Login>
* SAML_IDP_REDIRECTED_BROWSER_TO_SP: Redirected from IDP
* IDP_RESPONSE_XML:
PHNhbWxwOj11c3BvbWNIIElEPSjFOWM3MWU1ODYtYmYzYi00MTIhLTk3MDAtOTYwOTRlMDlmNmQzIiBWBXZXJzaw9uPSiYlJaiIElzc3VlSW5zdGFudD0iMjAy
* SAML_ERROR: Error receiving SgMl response 1
```

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*.
2. Click *Create > User*.
3. 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.
4. If desired, enable and configure the *Password* field. Users change their password during the activation process. You may want to configure a password if you anticipate that you need administrative access to this VPN user before the activation process.
5. 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 166](#).
6. Click *OK*.

See [Configuring a new service connection on page 52](#) 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 mode on page 9](#).

Profiles

FortiSASE supports multiple endpoint profiles to provide granular behavior for different groups of users, such as:

- IT can disconnect from always-on VPN.
- Marketing is allowed to use removable media and authenticates using LDAP.
- All other users cannot disconnect from always-on VPN, cannot use removable media, and authenticates using SSO.

In *Configuration > Profiles*, a table of profiles is presented, with the *Default* profile being assigned to all other users if no custom profiles have been defined. The *Default* profile cannot be deleted.

+ Create Edit Delete View Endpoints Search				
	Name	AD Users	AD Groups	Status
☐	FinanceEmployees		financial.local/Employees/Finance/Finance-Employees	✓ Enabled
☐	Default			✓ Enabled

Endpoint profiles can be prioritized and can be assigned to on-net endpoints based on matching Active Directory (AD) domain users and groups.

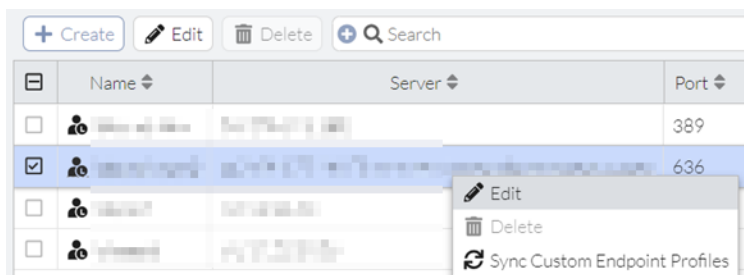
An LDAP server configuration is required to view users and groups from an AD server. LDAP user and group information is shared with the FortiSASE Endpoint Management service, which assigns profiles to endpoints that are locally connected to the LDAP domain whenever domain users are logged in by matching either selected users or selected groups.



If you have an existing LDAP server configured prior to FortiSASE 23.4, the custom endpoint profile cannot use it immediately. First, you must synchronize the LDAP server settings with the FortiSASE Endpoint Management Service using these steps:

1. From *Configuration > LDAP*, *Edit* the existing LDAP server.
2. Click *Back* twice to get back to the first page, *Set up server*.
3. On the *Set up server* page, click *Next*.
4. On the *Authenticate* page, select the *Bind* type, reenter the LDAP administrator credentials, and click *Next*.
5. On the *Review* page, click *Submit*.

From *Configuration > LDAP*, by right-clicking any LDAP server, you can synchronize custom endpoint profiles with any updates from the LDAP server, if necessary:



When creating a new endpoint profile, you can use the *AD Users & Groups* tab to select which AD users/groups the profile will apply to, and you can use an option in the *Access* tab to enable/disable single sign on (SSO) authentication per profile.

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. On the *Access* tab, configure the following:
 - 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 *Notify endpoint of VPN connectivity issues*. When enabled, a notification displays to the end user when FortiClient cannot connect to FortiSASE VPN.
 - c. Enable or disable *Authenticate with SSO*. When enabled and when SSO has been configured in *Configuration > VPN User SSO*, this endpoint profile uses SSO authentication. If SSO is not yet configured, a warning icon displays next to this setting to remind you to perform the required configuration.



FortiSASE supports authentication using multiple SSO providers using FortiTrust Identity. See [Configuring FortiSASE with FortiAuthenticator Cloud as SAML IdP proxy for Entra ID SSO on page 133](#).

- d. Enable or disable *Auto Connect to FortiSASE*. When enabled, FortiClient automatically connects to the FortiSASE VPN tunnel when the end user logs into the endpoint. The end user must have established connection to the FortiSASE VPN tunnel at least once before.
- e. Enable or disable *Force Always On VPN*. When enabled, the end user cannot manually connect or disconnect from FortiSASE.
- f. Under *Bypass FortiSASE*, 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. 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:
 - i. Click *Create*.
 - ii. Configure the following fields:

Option	Description
Type	Select <i>Infrastructure</i> , <i>FQDN</i> , <i>Local Application</i> , or <i>Subnet</i> .

Option	Description
Match	- If you selected <i>Infrastructure</i>, select the desired application from the dropdown list. - If you selected <i>FQDN</i>, enter 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 <i>Local Application</i>, 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 <i>Details</i> tab in Task Manager, add the <i>Image path name</i> column. - If you selected <i>Subnet</i>, 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 <i>Subnet</i> match type. You must create host groups in <i>Configuration > Hosts</i> before they become visible in the <i>Edit Match</i> dialog.



Subnet destinations cannot be created in a custom endpoint profile. Therefore, subnet destinations defined in the *Default* profile also apply to all custom profiles.

- iii. Click *OK*.
- g. Under *Bypass FortiSASE*, configure *Endpoints will not auto connect to VPN from these public IPs*. Endpoints with public IPs matching the configured public IPs are considered trusted or on-net, 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 optimize FortiSASE bandwidth usage. For example, when you add the public IP of your corporate network, the endpoints on this network will not automatically connect to FortiSASE VPN when they are on-net. Therefore, only when endpoints have public IPs that do not match the configured trusted public IPs will they auto connect to FortiSASE VPN, meaning when they are considered untrusted or off-net and require FortiSASE security inspection. Configure a public IP to prevent auto connect to FortiSASE VPN when endpoints are on-net:
 - i. Click *Create*.
 - ii. Enter the public IP address in the *Public IP* text field.
 - iii. Click *OK*.

5. On the *Protection* tab, 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 *Automatically Scan for Vulnerabilities*. FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities. You can view a summary of endpoint vulnerability information on the Dashboard.
- c. 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.
- a. Enable *Removable Media Access Control*. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.
 - i. Enable *Notify Endpoint of Blocks* to display a bubble notification when FortiClient takes action with a removable media device.
 - ii. 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 <i>Simple</i> or <i>Regex</i> for the rule type. When <i>Simple</i> is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions. When <i>Regex</i> 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: • <i>Allow</i>: Allow access to removable media devices connected to the endpoint that match this rule. • <i>Block</i>: 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.

iii. Click *OK*.

6. 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 <i>FortiSASE</i> to configure connection to FortiSASE Sandbox or <i>Standalone FortiSandbox</i> 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 <i>Quarantine</i> or <i>Alert & Notify</i> for infected files. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the <i>Sandbox Detection Verdict Level</i> setting.
Sandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the <i>Action</i> field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if <i>Action</i> is configured as <i>Quarantine</i> and <i>FortiSandbox Detection Verdict Level</i> is configured as <i>Medium</i> , 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 • Google • Skype

Options	Description
	• Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion list.

7. 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*.
8. On the *AD Users & Groups* tab, configure the AD users/groups to apply the endpoint profile to:



Viewing users and groups from an AD server requires an LDAP server configuration. See [Configuring FortiSASE with an LDAP server for remote user authentication in endpoint mode on page 118](#).



If you have an existing LDAP server configured prior to FortiSASE 23.4, the custom endpoint profile cannot use it immediately. First, you must synchronize the LDAP server settings with the FortiSASE Endpoint Management Service using these steps:

1. From *Configuration > LDAP*, *Edit* the existing LDAP server.
2. Click *Back* twice to get back to the first page, *Set up server*.
3. On the *Set up server* page, click *Next*.
4. On the *Authenticate* page, select the *Bind* type, reenter the LDAP administrator credentials, and click *Next*.
5. On the *Review* page, click *Submit*.

- a. By default, FortiSASE adds *Non-AD Groups* to the table. You may want to keep this group or select it and delete it accordingly.
- b. Click *Add* and select *AD Users* or *AD Groups*:
 - i. When selecting *AD Users*, a slide-in appears, which allows you to view the domains corresponding to configured LDAP servers. You can collapse the LDAP domain and select AD users from the list of users.
 - ii. When selecting *AD Groups*, a slide-in appears, which allows you to view the domains corresponding to configured LDAP servers. You can collapse the LDAP domain and select AD groups from a tree view of groups.
- c. Select *AD Users* or *AD Groups* from the respective slide-in.
- d. Click *OK*.

- e. Repeat steps b to d to add more AD users or groups.
- f. Click OK.

Example: Configuring a custom endpoint profile applied to an AD group

This example demonstrates how to configure a custom endpoint profile applied to an AD group. It demonstrates how to configure an LDAP server that allows group matching, how to configure a custom endpoint profile to use this LDAP server to select a specific AD group with which this profile will be applied, and how to test that the correct profile is applied to an AD user within the selected AD group.

This example makes the following assumptions:

- The LDAP server has already been configured with AD services, AD users and AD groups. Note that the AD user johnlocus is a part of the Finance-Employees AD group.
- SSO authentication has already been configured 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 LDAP server and joined to the LDAP domain.
- Default endpoint profile has been configured with Authenticate with SSO as Disabled to ensure LDAP is used for VPN user authentication.

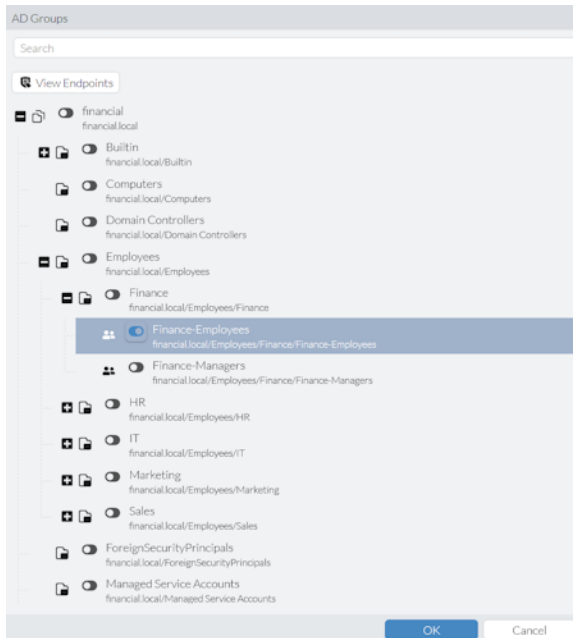
To configure an LDAP server:

1. Go to *Configuration > LDAP* and click *Create*.
2. Configure the LDAP server settings to match those on your LDAP server (modify these to match your setup):
 - a. *Server IP/Name*: < LDAP server IP/name >
 - b. *Server Port*: 389
 - c. *Common Name Identifier*: sAMAccountName
 - d. *Distinguished Name*: dc=financial, dc=local
 - e. *Secure Connection*: Disabled
 - f. *Advanced Group Matching*: Enabled
 - g. *Group Member Check*: User Attribute
 - h. *Group Filter*: < Empty >
 - i. *Group Search Base*: < Empty >
 - j. *Member attribute*: memberOf
3. Configure the bind type and administrator credentials:
 - a. *Bind Type*: Regular
 - b. *Username*: administrator@financial.local
 - c. *Password*: < Password >
4. Review the settings. Observe a notification that the LDAP server is successfully configured.
5. Click *Submit*.
6. Observe that a new LDAP server entry has been added to the table, noting that *Custom Endpoint Profiles* shows *Successful*.

To configure a custom endpoint profile applied to an AD group:

1. Go to *Configuration > Profiles* and click *Create*.
2. Add a name to the profile. For this example, use FinanceEmployees.

3. Go to the *Access* tab and configure these settings:
 - a. *Show tags on FortiClient*: Enabled
 - b. *Notify endpoint of VPN connectivity issues*: Enabled
 - c. *Authenticate with SSO*: Enabled
 - d. *Auto Connect to FortiSASE*: Enabled
 - e. *Force Always On VPN*: Disabled
4. Go to the *AD Users & Groups* tab to configure the AD group that the custom endpoint profile will apply to:
 - a. Select *Non-AD Groups* and click *Delete*. Click *OK* to confirm the deletion.
 - b. Click *Add > AD Groups*.
 - c. Collapse the LDAP domain and select the desired AD group.



- d. Click *OK*.
- e. Review the selected AD group.
- f. Click *OK*.
- g. 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*, select the custom endpoint profile just created, and click *View Endpoints*. The *Managed Endpoints* view filtered with endpoints using the selected profile displays.

Endpoint	Profile	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPI
Windows-User-2	FinanceEmployees	johnlocus		Online			Discon

3. Alternatively, you can view all endpoints with different profiles using *Network > Managed Endpoints* under the *Endpoints* tab.

Endpoints

Software Installations

View Endpoint Details

Management Connection

More Options

Managed Endpoints

Unmanaged Endpoints

Search filterable columns

	Endpoint	Profile	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPN
☐	 WinDev2310Eval	Default	 User	johnlocus	 Online	Ashburn - Virginia - USA	104.134.130.130	 Connect
☐	 Windows-User-2	FinanceEmployees	 johnlocus		 Online		104.134.130.130	 Disconnect

- Establish a VPN connection on the test endpoint using SSO authentication.
- 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.

Endpoints

Software Installations

View Endpoint Details

Management Connection

More Options

+

Search filterable columns

Managed Endpoints

Unmanaged Endpoints

	Endpoint	Profile	Device Username	VPN Username	Management Connection	Security PoP	Public IP	VPN
☐	 WinDev2310Eval	Default	 User	johnlocus	 Online	Ashburn - Virginia - USA	104.134.130.130	 Connect
☐	 Windows-User-2	FinanceEmployees	 johnlocus	@azure.kldo...	 Online	Ashburn - Virginia - USA	104.134.130.130	 Connect

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:

- FortiSASE sends tagging rules to endpoints.
- FortiClient checks endpoints using the provided rules and sends the results to FortiSASE.
- FortiSASE receives the results from FortiClient.
- 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 161](#) 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:

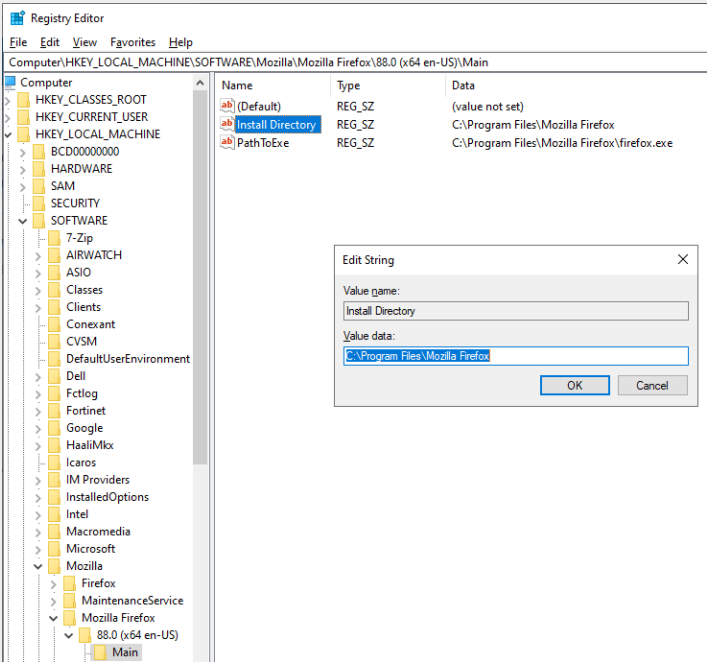
1. Configure the tagging rule set:
 - a. Go to *Configuration > ZTNA Tagging*. Click the *ZTNA Tagging Rules* tab, then click *Create*.
 - b. In the *Name* field, enter the desired rule set name.
 - c. Toggle *Enabled* on or off to enable or disable the rule.
 - d. (Optional) In the *Comments* field, 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 access 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 <i>User in AD Group</i> dropdown list, select the desired Active Directory (AD) group that users should be members of. You can also use the <i>Negate</i> 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.

Rule type	OS	Description
AntiVirus	- Windows - macOS - Linux	From the <i>AntiVirus</i> 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 <i>Negate</i> 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 <i>Subject CN</i> and <i>Issuer CN</i> fields, enter the certificate subject and issuer. You can also use the <i>Negate</i> 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 <i>Domain</i> 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.
File	- Windows - macOS - Linux	In the <i>File</i> field, enter the file path. You can also use the <i>Negate</i> 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 <i>IP Range</i> 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.

Rule type	OS	Description
Operating System Version	- Windows - macOS - Linux - iOS - Android	From the <i>Operating System Version</i> 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.
Registry Key	Windows	In the <i>Key</i> field, enter the registry path or value name. End the path with <code>\</code> to indicate a registry path, or without <code>\</code> to indicate a registry value name. You can also use the <i>Negate</i> 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 <code>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main</code>. The value name is <code>Install Directory</code>, and the value data is <code>C:\Program Files\Mozilla Firefox</code>. You can configure a registry key rule to match <code>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main</code> as the path or <code>Install Directory</code> as the registry value name, but you cannot configure a rule to match <code>C:\Program Files\Mozilla Firefox</code>.  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.

Rule type	OS	Description
Running Process	- Windows - macOS - Linux	In the <i>Process Name</i> field, enter the process name. You can also use the <i>Negate</i> 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 <i>Sandbox Detection</i> 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 <i>Negate</i> 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 <i>Severity Level</i> dropdown list, select the desired vulnerability severity level.
User Identity	- Windows - macOS - Linux - iOS - Android	Under <i>User Identity</i>, select the following: <i>User Specified</i>: endpoint user manually entered their personal information in FortiClient. <i>Social Network Login</i>: endpoint user provided their personal information by logging in to their Google, LinkedIn, or Salesforce account in FortiClient. You can further select one of the following: <i>All Accounts</i>: all endpoints where the user logged in to the specified social network account type. <i>Specified</i>: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter <code>joanexample@gmail.com</code> 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 <i>Negate</i> 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 <i>Windows Security</i> 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 <i>Negate</i> 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.

System

Certificates

You can upload a certificate for use with SSL deep inspection, and LDAP and SAML SSO authentication.

To upload a certificate:

1. Go to *System > Certificates*.
2. Click *Import*, then select *CA Certificate* or *Remote Certificate*.
3. Configure the fields and upload the certificate and key files as needed.
4. Click *OK*.

HTML Templates

You can customize block pages that display on endpoints in certain situations, such as if FortiSASE has blocked access based on Application Control With Inline-CASB settings. 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 administration 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>%%`. In this example, it is replaced 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 is blocking access to.

The screenshot shows the FortiSASE Application Control Block Page. The page title is "FortiSASE - Secure Internet Access". Below the title, it says "Application Blocked" and "You have attempted to use an application that violates your Internet usage policy. Call 555-555-5555 for assistance." A table lists the blocked application details:

Application	Facebook
Category	Social Media
URL	http://www.example.com/
Username	Guest
Group Name	Guest-group
Policy	35ef0f54-35d5-51e3-ae02-3d6776b41e4d

On the right side of the page, there is a CSS code editor showing the following code:

```

52 border-radius: 3px;
53 min-width: 6em;
54 font-weight: 400;
55 font-size: 0.8em;
56 cursor: pointer;
57 }
58
59 button.primary {
60   color: #fff;
61   background-color: rgb(47, 113, 178);
62   border-color: rgb(34, 103, 173);
63 }
64
65 .message-container {
66   height: 500px;
67   width: 600px;
68   padding: 0;
69   margin: 10px;
70 }
71
72 .logo {
73   height: 80%;
74   background: url(%%IMAGE:font%%) no-repeat left bottom;
75   background-size: 65px;
76 }
77
78 table {
79   background-color: #fff;
80   border-spacing: 0;
81   margin: 1em;
82 }
83
84 table > tbody > tr > td:first-of-type:not([colspan]) {
85   white-space: nowrap;
86   color: rgba(0, 0, 0, 0.5);
87 }
88
89 table > tbody > tr > td:first-of-type {
90   vertical-align: top;
91 }
92
93 table > tbody > tr > td {
94   padding: 0.3em 0.3em;
95 }
96
97 .field {
98   display: table-row;
99 }
100
101 .field > :first-child {
102   display: table-cell;
103   width: 20%;
104 }
105
106 .field.single > :first-child {
107   display: inline;
108 }

```

At the bottom of the page, there are buttons for "Restore Defaults", "Save", and "Cancel".

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. 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 89](#).

SECURE WEB GATEWAY CONFIGURATION

Enable

☒

Global (Recommended)



Secure Web Gateway Server(s)

Canada West (Burnaby)



Canada East (Ottawa)



US-East-1 (Ashburn)



United Kingdom (London)



Secure Web Gateway Port

PAC File

 Download

Hosted PAC File



OK

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 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 will use 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. Click *OK*.
7. 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

The following lists the type of reports 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 accessed by the user and applications.
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, 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.
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 collected 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 SSL 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 top bandwidth usage. Also identifies users who are blocked the most from websites.

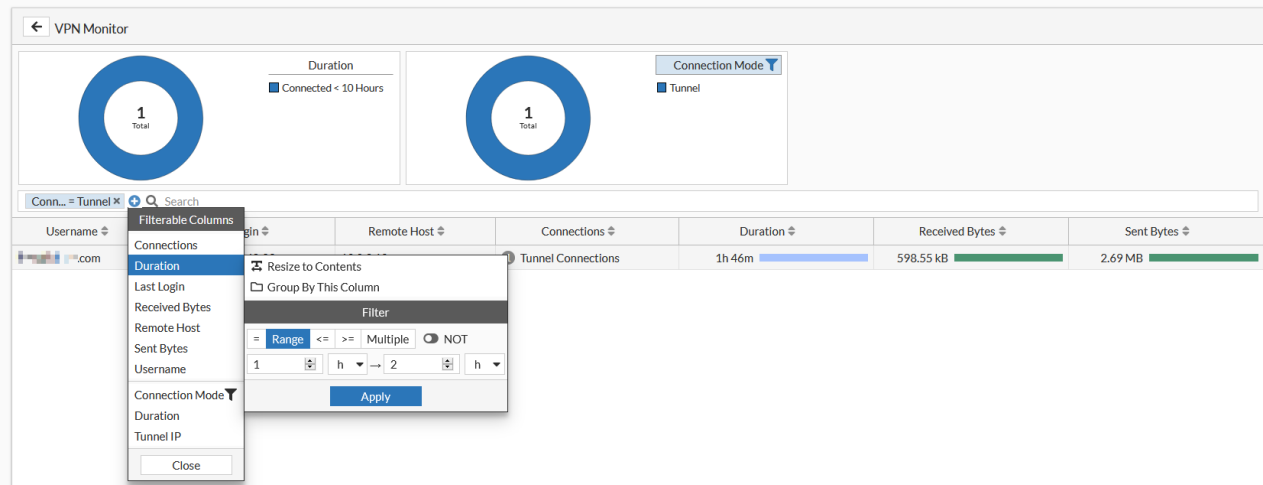
Logging

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

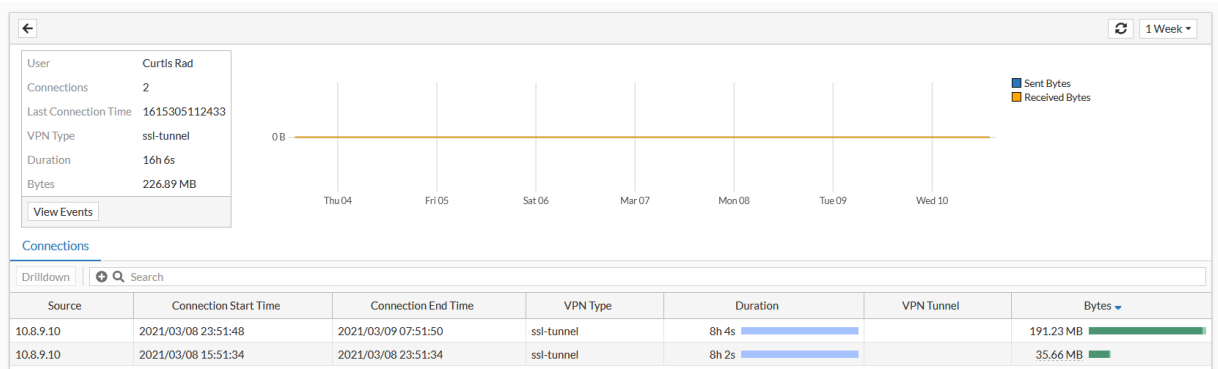
others.

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.

Date/Time	Application Name	Security Events	Action	Security Action	Result
2021/03/10 13:52:47	PS.BROWSER		✓ Accept	✓ Allowed	✓ 3.53 kB / 5.65 kB
2021/03/10 13:52:42			✓ Accept		✓ 156 B / 268 B
2021/03/10 13:51:47	PS.BROWSER		✓ Accept	✓ Allowed	✓ 3.53 kB / 5.67 kB
2021/03/10 13:51:42			✓ Accept		✓ 156 B / 268 B
2021/03/10 13:50:52			✓ Accept		✓ 3.11 kB / 5.45 kB

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*.
3. From *Remote Server Type*, select *FortiAnalyzer*, *Syslog*, or *Common Event Format (CEF)*.
4. In the *Server Address* and *Server Port* fields, enter the desired address and port for FortiSASE to communicate with the server.
5. Enable *Reliable Connection* to use TCP for log forwarding instead of UDP.
6. 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 in order for the TLS connection to be successful by clicking on the *Certificates* button.

Alternatively, go to *System > Certificates*.

- For details on importing a Remote CA certificate, please refer to [Certificates on page 166](#).
- For details on the cipher suites that are supported for a secure external syslog server, see [Supported cipher suites for secure external syslog server](#).

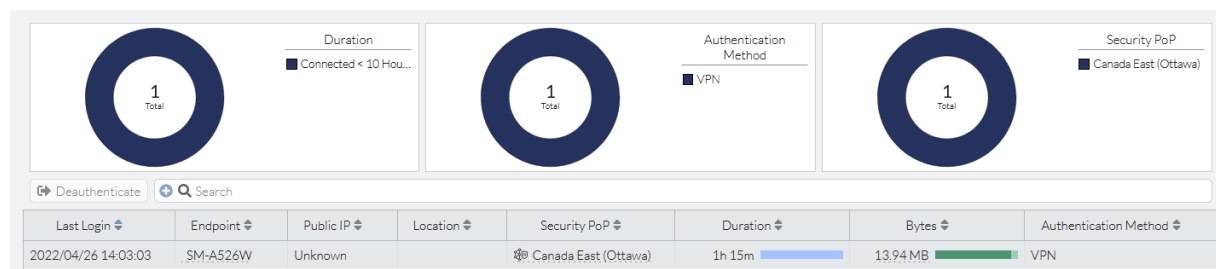


The remote CA certificate for the external syslog server must be imported to FortiSASE, to establish trust with the external syslog server. Otherwise, the TLS connection will not be successful and logs forwarded will not be readable by the external syslog server.

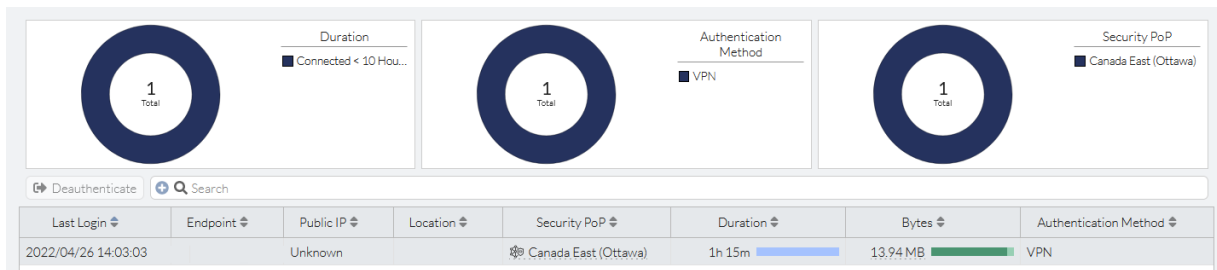
Log anonymization

Log anonymization allows you to hide personally identifiable user information, such as their hostname and avatar, in Dashboard widgets, logs, and other areas of FortiSASE.

The following shows the *Connected Users* page when log anonymization is disabled. The hostname information is visible.



The following shows the Connected Users page when log anonymization is enabled. The hostname information is no longer visible.



The following shows log anonymization's effect on *Analytics > Logs > Traffic*. In the following example, all logs are from the same source, dcat@fortinet.com, and log anonymization was enabled at 10:31. All logs for traffic that occurred before 10:31 show the source information, dcat@fortinet.com. All logs that occurred after 10:31 have the source information anonymized.

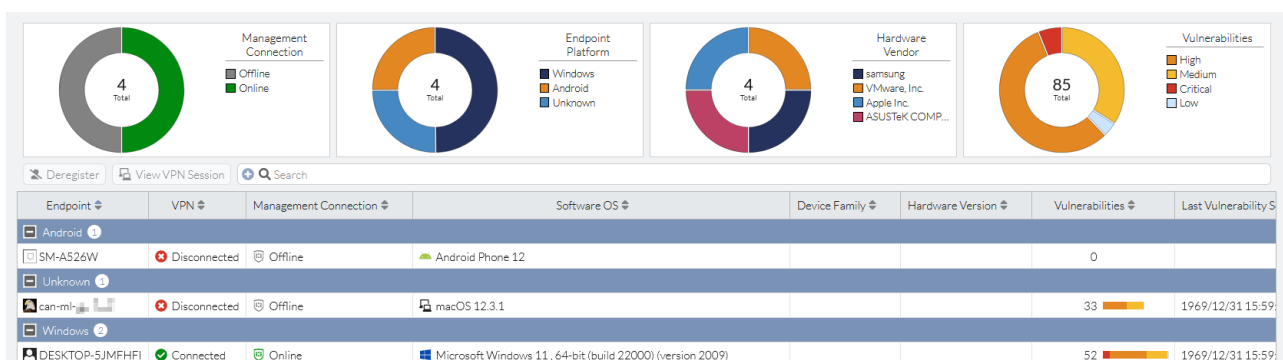
You cannot retroactively anonymize or deanonymize source information by enabling or disabling anonymization. The source information remains anonymized or not anonymized based on whether log anonymization was enabled or disabled when the traffic occurred.

← Outbound Traffic

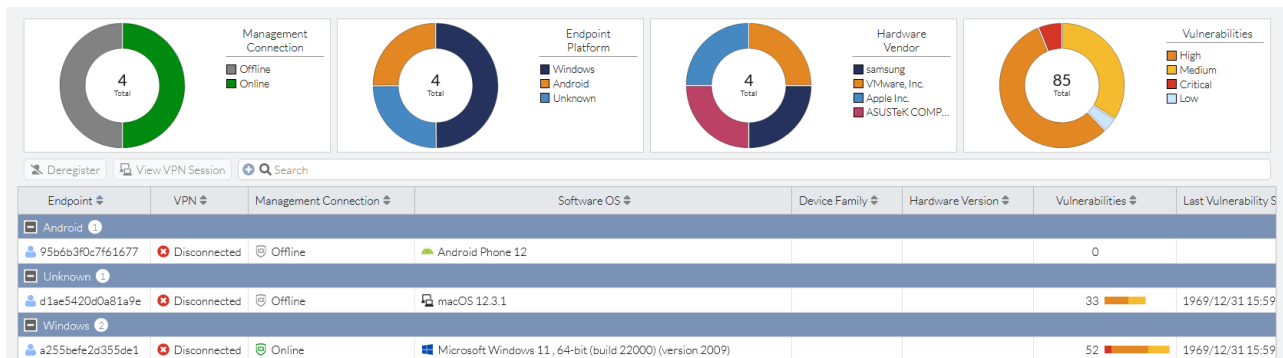
🔄 ⬇️ 🔍 Search

Date/Time	Source	Destination IP	Application Name	Policy ID	Security Events	Action	Security Action	Result
2022/04/27 10:31:24	93c29826e5166a7c	172.217.14.206 (sea30s01-in-f14.1e100.net)	YouTube	3	Web Filter Application Control	TCP reset from client	Blocked	Deny: UTM Blocker
2022/04/27 10:31:23	93c29826e5166a7c	172.217.14.206 (sea30s01-in-f14.1e100.net)	SSL	3	Application Control	TCP reset from client	Allowed	UTM Allowed
2022/04/27 10:31:23	93c29826e5166a7c	172.217.14.206 (sea30s01-in-f14.1e100.net)	SSL	3	Web Filter Application Control	TCP reset from client	Blocked	Deny: UTM Blocker
2022/04/27 10:31:20	93c29826e5166a7c	208.91.114.120	Fortinet-Other	3		Accept: session close		0 B / 21.53 kB
2022/04/27 10:31:18	93c29826e5166a7c	44.225.152.184 (forticlient-emspoxy.forticloud.com)	HTTPS.BROWSER	3	Application Control	TCP reset from server	Allowed	UTM Allowed
2022/04/27 10:30:52	dcat@fortinet.com	172.16.208.233	DNS	3		Accept		315 B / 0 B
2022/04/27 10:30:49	dcat@fortinet.com	209.121.79.107 (s209-121-79-107.bc.hsia.telus.net)	DNS	3		Accept		144 B / 192 B
2022/04/27 10:30:43	dcat@fortinet.com	209.121.79.107 (s209-121-79-107.bc.hsia.telus.net)	DNS	3		Accept		63 B / 214 B
2022/04/27 10:30:43	dcat@fortinet.com	209.121.79.107 (s209-121-79-107.bc.hsia.telus.net)	DNS	3	DNS Filter	Accept		68 B / 127 B

The following shows the Managed Endpoints page when log anonymization is disabled. The hostname information is visible.



The following shows the Managed Endpoints page when log anonymization is enabled. The hostname and avatar is anonymized. All endpoints also display as being disconnected from VPN.



When log anonymization is enabled, VPN appears as disconnected for all endpoints to ensure anonymity.



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 > LOGS > 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 174](#).

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

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).

For existing FortiSASE instances, this feature remains disabled by default, which allows a default log retention period of 60 days until you explicitly configure this setting. New FortiSASE instances have a log retention period of 30 days by default. You can configure the log retention policy to between a minimum of 2 days to a maximum of 30 day, and it 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 171](#).

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.

Client onboarding

Client using managed endpoints connect using VPN. You can onboard them using the *Onboard Users* slide-in page.

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 11](#) describes.

The screenshot shows a dashboard with two main sections. On the left, under 'Health Status', there is a table with components and their status:

Component	Status
FortiSASE Network (AS40...)	Operational
FortiSASE Cloud Regions	Operational
FortiSASE Services	Operational

Below this table is a 'More Information' button. On the right, under 'Remote Users', there is a table with entitlements and current usage:

Entitlement	Value
Endpoints	100
FortiSASE users	100
FortiCASB users	100
License expiry	2023/05/17
Current Usage	
Connected users	0

An 'Onboard Users' button is located at the top right of the 'Remote Users' section.

- Go to *Configuration > Users* and click *Onboard Users* at the top right of the page.

The screenshot shows the 'Users' configuration page. At the top, there are buttons for 'Create', 'Edit', 'Delete', and a search bar. Below the buttons is a table with columns for 'Name', 'Details', and 'References'.

Name	Details	References
User		
user1@ft.com		2
user2@ft.com		2
test@test.com		2
User Group		
aaa	user1@ft.com, user2@ft.com, test@test.com	5

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 176](#).
- Secure Web Gateway Users. See [SWG client onboarding on page 178](#).

Managed endpoint client onboarding

Onboard Users > Managed Endpoint Users includes features to support onboarding managed endpoint clients.

Managed Endpoint Users

To connect to FortiSASE, users will need to input the invitation code below into FortiClient:

Invitation Code

Preconfigured FortiClient Installers   Windows x86/x64  MacOS

Generic FortiClient Installers   Linux  IOS  Android

Invite Users

You can include the emails of users you would like to be onboarded to FortiSASE. The invitation email includes FortiClient download links and the invitation code.

Feature	Description
Invitation Code	This is the code to input into FortiClient to allow managed users to be automatically provisioned to connect to FortiSASE. In FortiClient, on the <i>Zero Trust Telemetry</i> tab, input the invitation code from FortiSASE in the <i>Register with Zero Trust Fabric</i> field, and click <i>Connect</i>.
Preconfigured FortiClient Installers	These installers are preconfigured with your FortiSASE invitation code. Clicking a preconfigured installer for a supported operating system downloads the installer to your local machine. You can then provision your endpoints by doing one of the following: - Using a mobile device management (MDM) software suite using this installer - Distributing this installer to end users and having them install it on their endpoints
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 operating system goes to a download page where you can select and download the installer to your local machine. Whether you decide to provision your endpoints using this installer and an MDM, or distribute this installer to end users, end users must input the invitation code that you provide for your FortiSASE instance.
Invite Users	Click + to add a blank field where you can enter the email address of the managed endpoint users to onboard to FortiSASE. Click + as many times as desired to enter email addresses. When you complete entering the email addresses of managed endpoint users, click <i>Send</i>. This feature sends an invitation email to the specified users which includes the generic FortiClient installer download links and invitation code.

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.

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.

Please note that 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 178](#).

```
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-hqwdvql7.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.

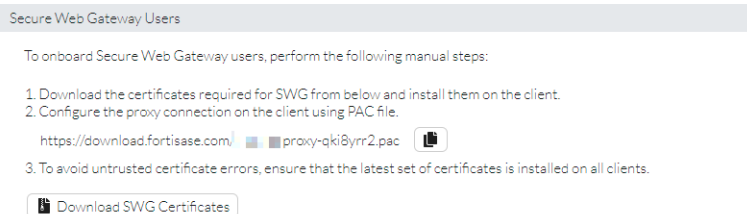
For details on downloading and installing the SWG certificate on an endpoint, refer to the steps in [Certificate installation on page 183](#).

For details on configuring the endpoint to use the custom hosted PAC file, refer to the steps in [Proxy configuration on page 186](#).

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 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.



The following instructions demonstrate installing certificates on various operating systems:

- [Windows on page 183](#)
- [macOS on page 184](#)
- [Chrome OS on page 184](#)
- [Managed Chromebook on page 185](#)

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*.

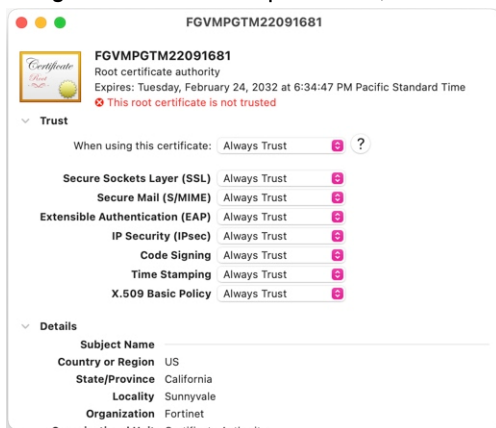
5. Review and click *Finish* to install the certificate.

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*.

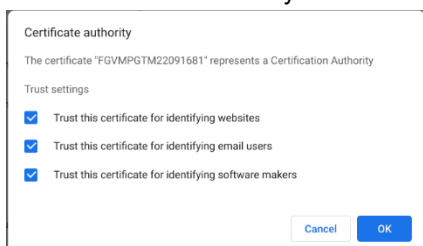


4. Save the configuration and add the certificate to the system keychain. You can connect to HTTPS websites without seeing a warning.

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*.

× Add certificate

Certificate
Applied at PowerUsers

Name
FortiSASE-CA

File attached
Fortinet_CA_SSL.cer ×

Issued to: FGVMPGTM22091681, Certificate Authority, Fortinet
Issued by: FGVMPGTM22091681, Certificate Authority, Fortinet
Issue date: February 23, 2022
Expiry date: February 24, 2032

Certificate Authority

Use as a Certificate Authority for the following

1 HTTPS security may be severely compromised if the private key portion of this certificate isn't stored securely.

☐ Android
☒ Chromebook
☐ iOS
☐ Imprivata App on Chromebooks
☐ Endpoint Verification

1 You need to enable advanced mobile management to apply the Android and iOS settings. [ENABLE ADVANCED](#)

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.

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 167](#).

Users are expected to have installed the FortiSASE certificate authority certificate on their devices. See [Certificate installation on page 183](#).

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 186](#)
- [macOS on page 187](#)
- [Chrome OS on page 188](#)
- [Managed Chromebook on page 189](#)

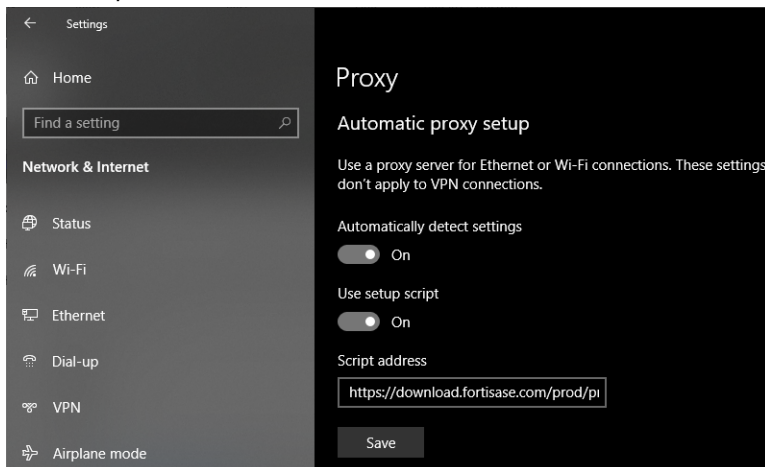
Windows

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*.



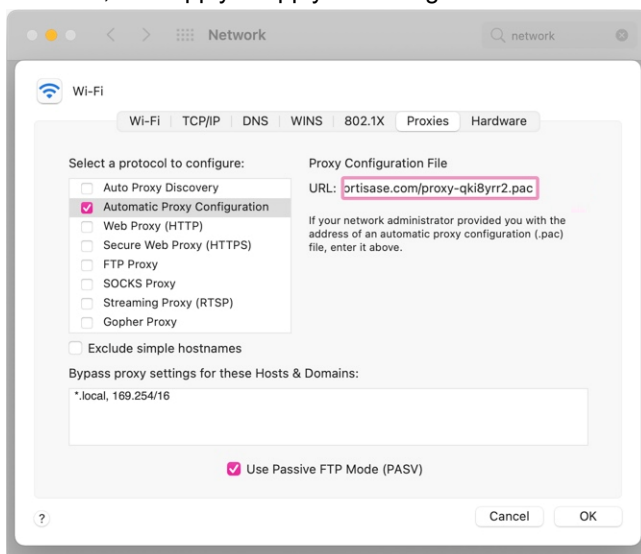
4. The next time the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE credentials in the prompt. After ten minutes of inactivity, the browser reprompts for authentication credentials.

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.

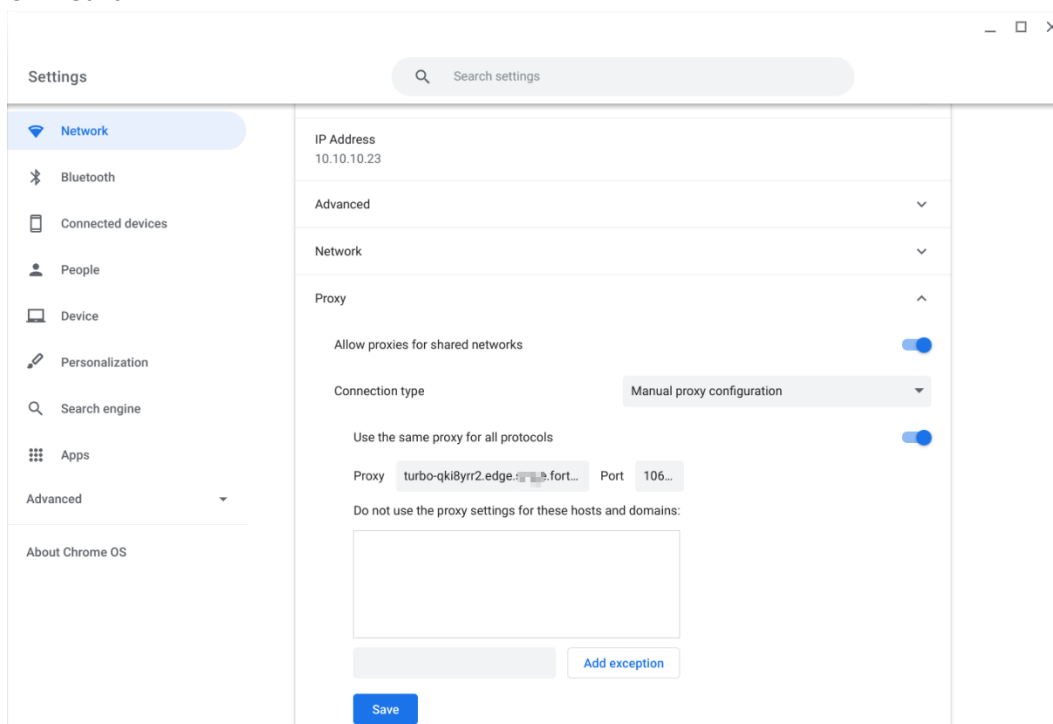


- The next time that the user starts a browser session, the browser displays an authentication prompt. The end user enters their FortiSASE user credentials in the prompt to authenticate.

Chrome OS

To configure proxy as a system-wide setting:

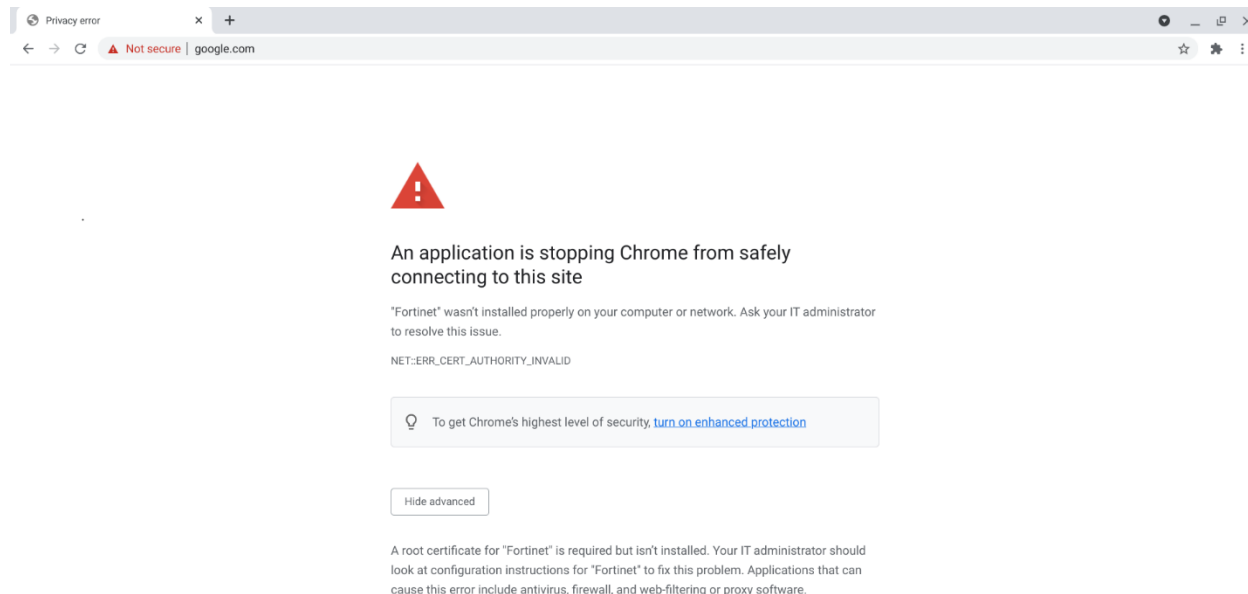
- Open the Launcher, and search for *Settings*.
- Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
- Scroll to the bottom and expand the proxy settings.
- For *Connection type*, select one of the following:
 - Select *Automatic proxy configuration*. This is the recommended method. Point the *Autoconfiguration URL* to the FortiSASE-hosted PAC file.
 - To configure manual proxy configuration, do the following:
 - Select *Manual proxy configuration*.
 - Enable *Use the same proxy for all protocols*.
 - 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.
 - 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.

- On a successful connection, your browser prompts you to authenticate. Enter your user credentials to authenticate to FortiSASE 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.

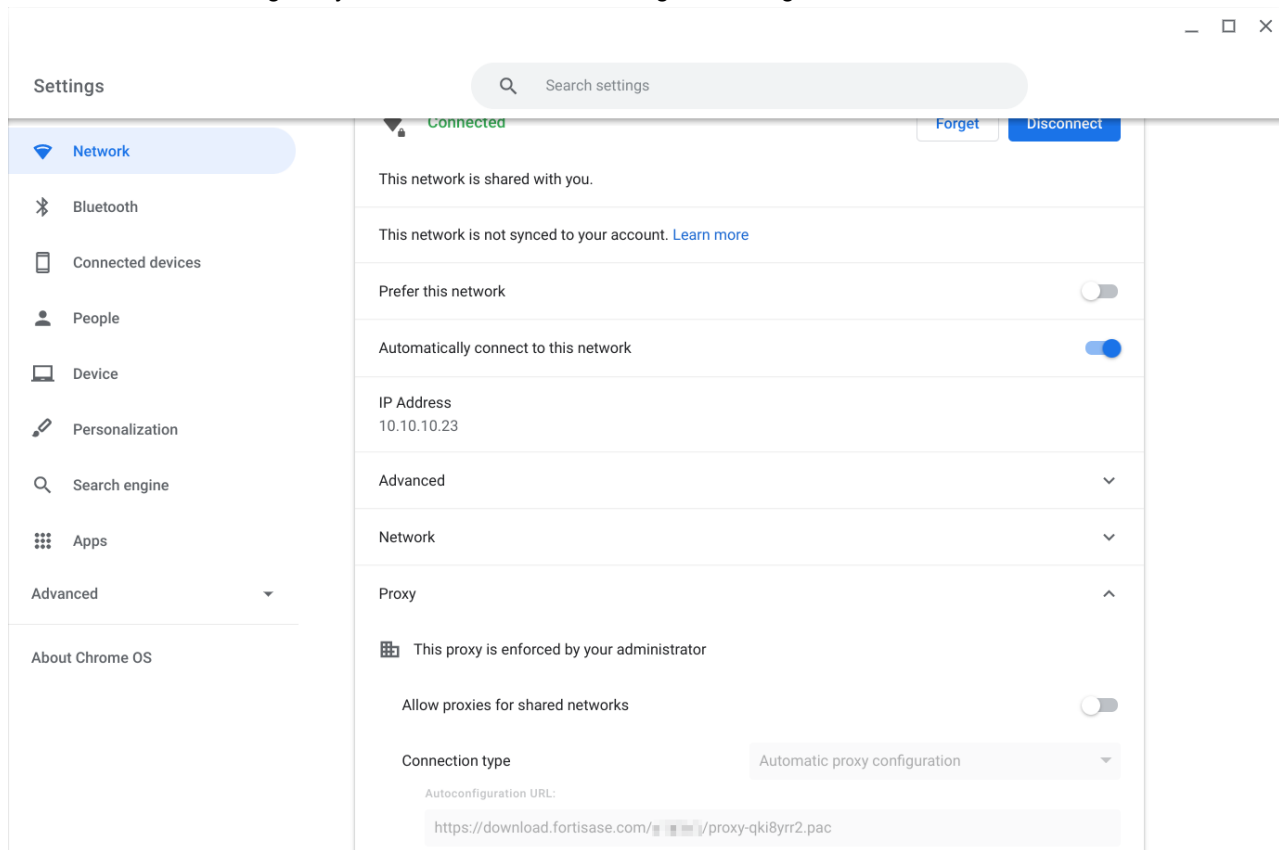
To configure proxy as a system-wide setting on Google Admin Console:

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:

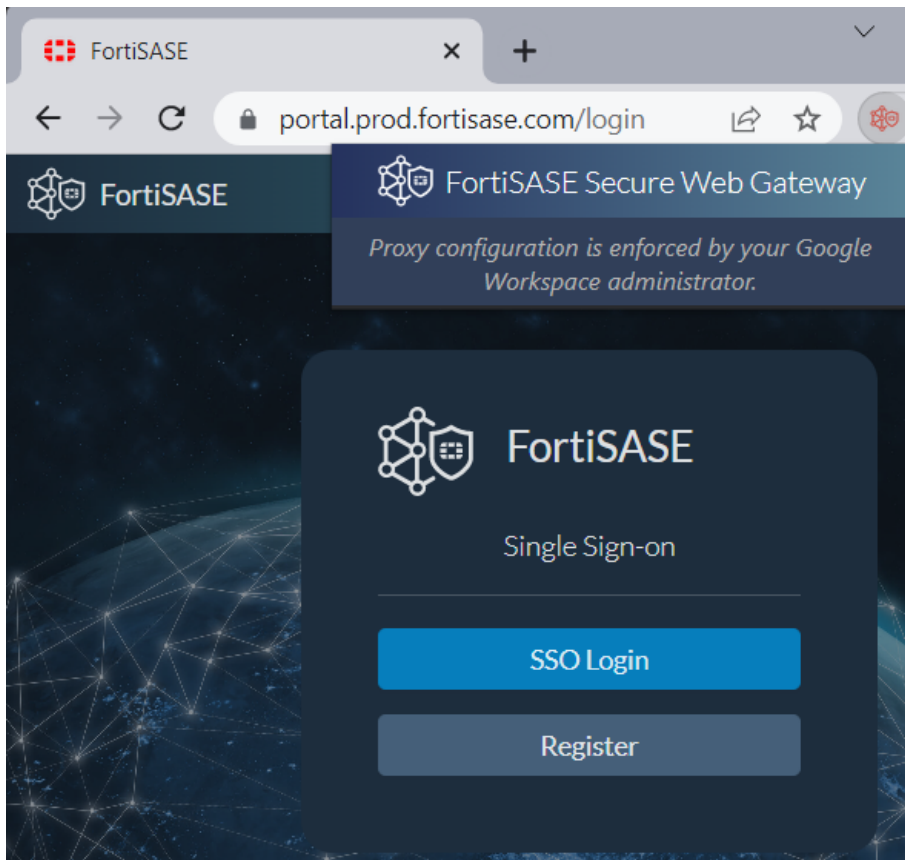
1. Open the Launcher and search for Settings.
2. Click *Network* on the left menu. Then select your Wireless Network SSID and click the right arrow to expand.
3. Scroll to the bottom and expand the proxy settings. The settings pushed from the Google Admin Console appear

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.



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 183](#) 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:

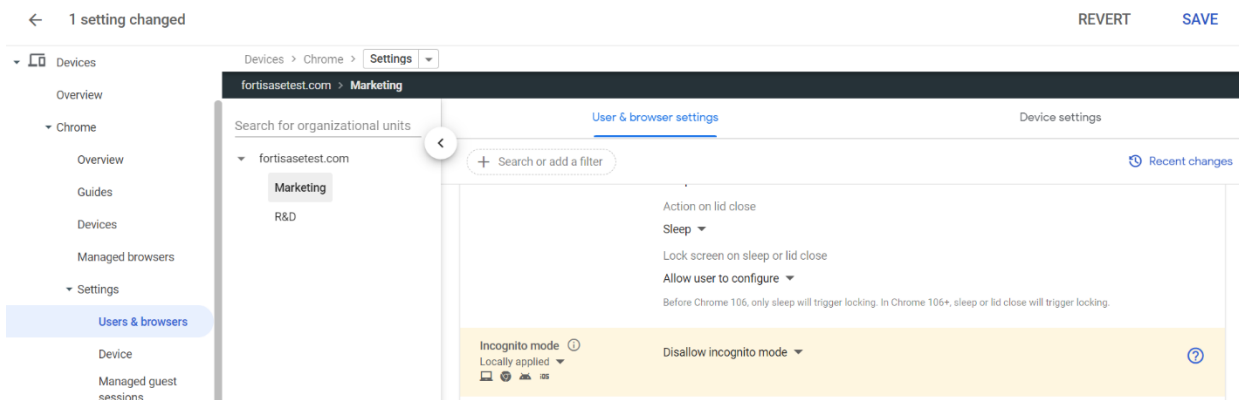
- Default or custom hosted PAC file URL
- User ability to view PAC file URL within the extension
- Configuration of supported platforms (ChromeOS, Linux, macOS, and Windows) where SWG is enforced

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 `aecejhdejcfnfihadbfdmndehobfdpcc`.
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
<code>pacFileUrl</code>	PAC file that the extension will enforce. Configure one of the following: - Default hosted PAC file link from FortiSASE in <i>System > SWG Configuration</i>. See SWG Configuration on page 167. - Custom hosted PAC file link from a server accessible to endpoints. See PAC file customization on page 178.
<code>showProxyInfo</code>	Possible values: <code>false</code> or <code>true</code> . - Setting this to <code>false</code> hides the PAC file URL from the extension. - Setting this value to <code>true</code> makes the PAC file URL visible to the extension.
<code>supportedPlatforms</code>	Possible values include <code>cros</code> , <code>linux</code> , <code>mac</code> , and <code>win</code> 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 <code>supportedPlatforms</code> array - Set <code>pacFileUrl</code> to an empty string - Remove the <code>pacFileUrl</code> 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.

[Home](#) > [Apps](#) | [App configuration policies](#) > [jaguar test](#)

jaguar test | Properties

Search

Overview

Manage

Properties

Monitor

Device install status

User install status

Basics Edit

Name	jaguar test		
Description	--		
Device enrollment type	Managed devices		
Platform	iOS/iPadOS		
Targeted app	FortiClient		

Settings Edit

Configuration key	Value type	Configuration value
cloud_invite_code	String	DTUE5H1BDQWSMKSCJJRN2FOKAG65808M

Assignments Edit

Included groups

Group	Filter	Filter mode
All users	None	None
All devices	None	None

Excluded groups

Group
No results.

Deploying trusted certificates

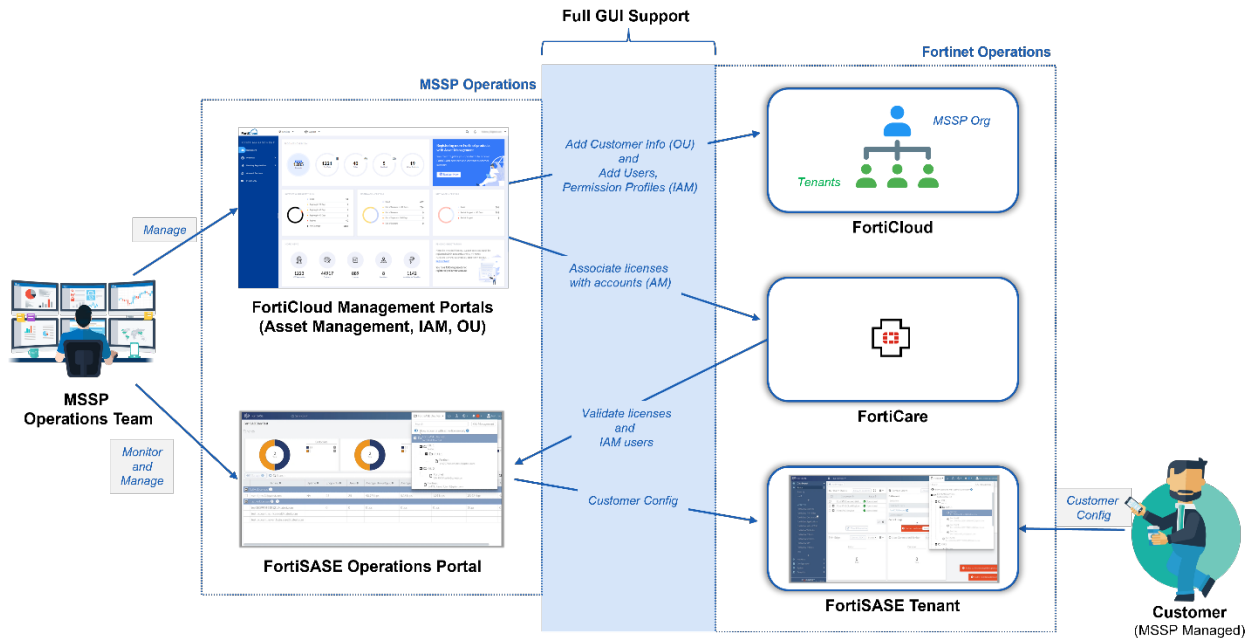
When FortiSASE security components are configured to use SSL deep inspection, then the certificate authority (CA) certificate is automatically installed on desktop FortiClient endpoints. However, for mobile endpoints such as Apple devices running FortiClient iOS, then enterprise mobility management software 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. Invite FortiCloud accounts to join OUs. See [Invitations](#) and [Creating invitation tokens](#).
 - e. Approve invitations to FortiCloud accounts. See [Invitation Approval](#) for details.
2. Using the FortiCloud IAM portal:
 - a. Set up a permission profile allowing IAM users to access FortiSASE as a portal. Permission control is global to the FortiSASE portal and provides the following roles:
 - No access
 - Read/write access
 - Read-only accessSee [Permission profiles within Organizations](#).
 - 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 198](#).
 - c. Monitor tenants' FortiSASE instances. See [Monitoring a tenant's instance on page 199](#).
 - d. Manage tenants' FortiSASE instances. See [Managing a tenant's instance on page 200](#).

For details on configuring FortiCloud OUs and adding FortiCloud accounts to OUs, see [Organization Portal](#).

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.

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 198](#).
3. Monitor the status of a tenant's FortiSASE instance. See [Monitoring a tenant's instance on page 199](#).

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 200](#).

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.

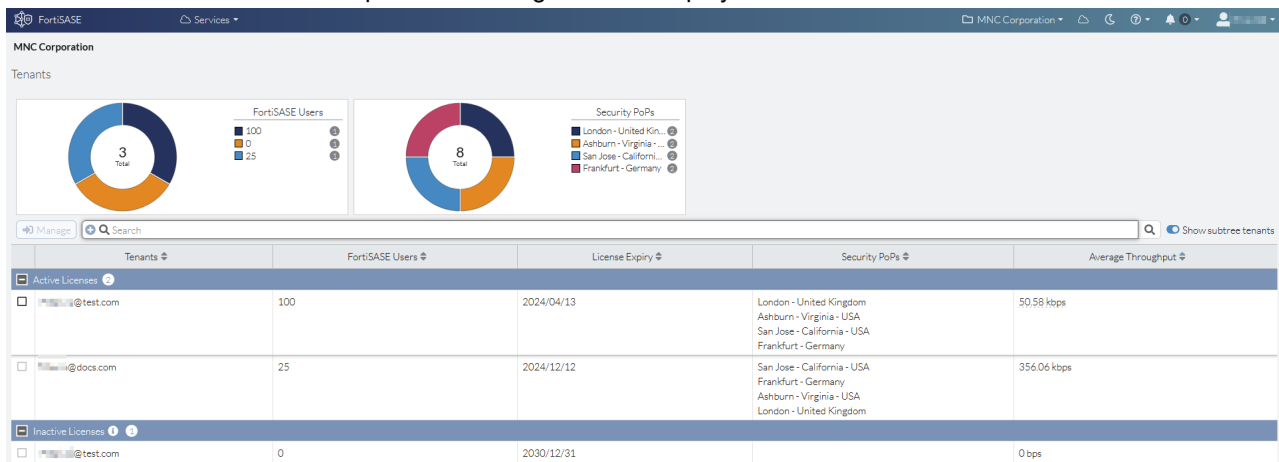


When configuring IAM users for an organization, you typically configure the user type as *Organization* with a *Permission Scope* configured to an organization unit (OU) or sub-OU. These users can access the MSSP portal.

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.

To access the MSSP portal from the FortiSASE portal:

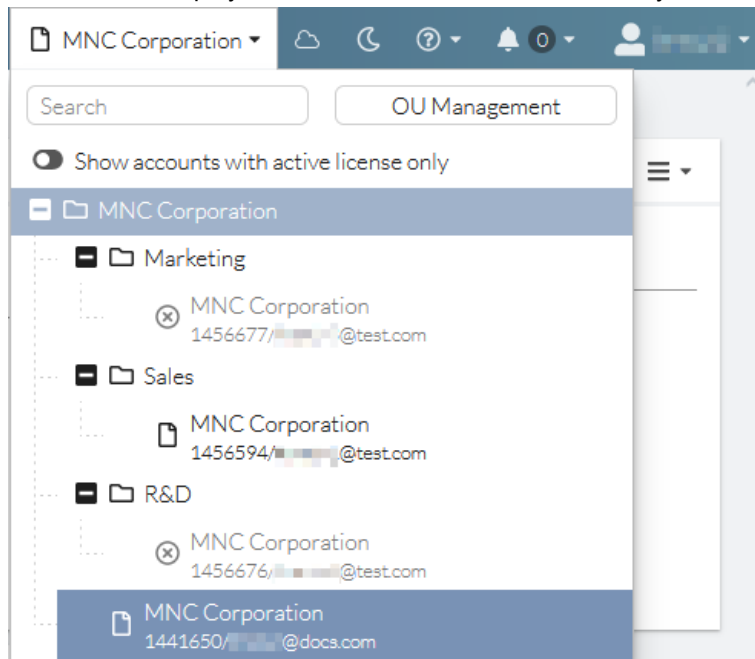
1. Go to the [FortiSASE portal](#).
2. Click *SSO Login*.
3. Click *Sign in as IAM user*.
4. Log in with the user credentials from the CSV that you downloaded when creating the IAM user in [To create an IAM user with the wizard](#). The MSSP portal for the organization displays.



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:

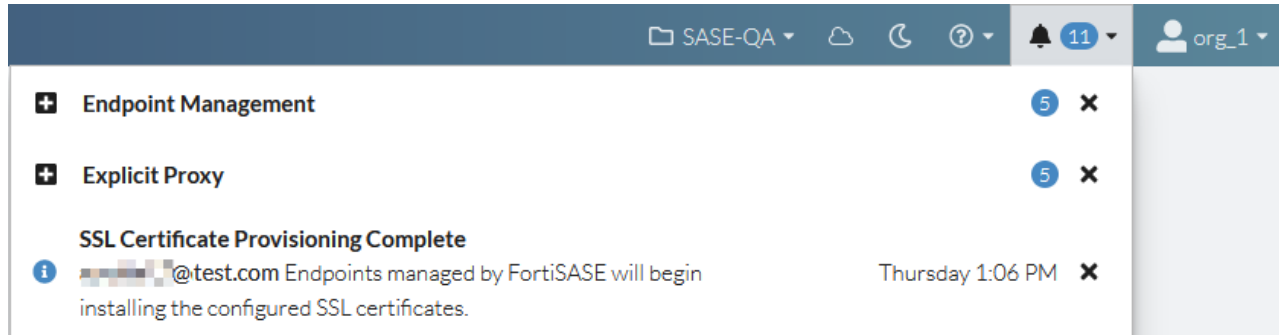
- Pie charts showing the distribution of FortiSASE users for active and inactive licenses and the distribution of security points of presence (PoP)
- Tenant entries separated into *Active Licenses* and *Inactive Licenses* categories. The *Inactive Licenses* category is for tenants for which data is not 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.

To manage a tenant's FortiSASE instance from the MSSP portal using the Manage button:

- From the MSSP portal, in the *Active License* category, click a tenant.
- Click *Manage*.
- 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.
- 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:

- From within a FortiSASE instance, select the context switch dropdown menu. Accounts within the organization display.
- Enable *Show accounts with active license only* to filter the dropdown menu to only display organization units and IAM users with active licenses.
- Select the IAM user whose FortiSASE instance you want to manage.
- The tenant's FortiSASE instance as if you had logged into the FortiSASE portal using the IAM user account associated with the instance.
- Perform any configuration within the FortiSASE instance with the same permissions as the IAM user account associated with the instance.

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](#).

Appendix A - FortiSASE data centers

The following provides information about FortiSASE data centers available through the FortiSASE Status page, global data centers list, and egress IP addresses feed.

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>.

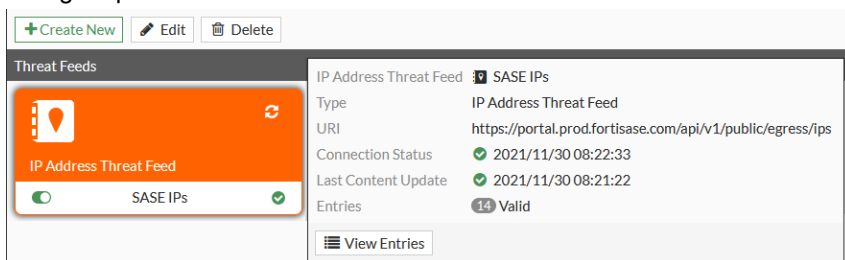
You can use this list in access control lists to allow access to internal applications from FortiSASE only.

The following describes how to configure a threat feed using this feed in FortiOS. For more 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 *URI 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.



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 202](#) via `ping`, `tracert`, 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](#).

You may want to consider enabling DTLS in FortiSASE to resolve increase latency. This feature is currently opt-in only and requires a FortiCare ticket. Reference bug ID 778651 when submitting a ticket.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.