

# Release Notes

FortiSASE 25.2.30



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



May 26, 2025

FortiSASE 25.2.30 Release Notes

72-25230-1150721-20250526

# TABLE OF CONTENTS

<b>Change log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>What's new</b>	<b>7</b>
What's new for 25.2.30 (25.2.a.1)	7
What's new for 25.2.24 (25.2.a)	7
What's new for 25.1.75 (25.1.c)	8
What's new for 25.1.51 (25.1.b)	8
What's new for 25.1.39 (25.1.a.2)	9
What's new for 25.1.37 (25.1.a.1)	9
What's new for 25.1.28 (25.1.a)	9
<b>Special notices</b>	<b>11</b>
On-shore Dubai customers	11
Removable media access	11
Activating the FortiClientNetwork extension	11
<b>Select availability features</b>	<b>13</b>
<b>Beta features</b>	<b>14</b>
<b>Product integration and support</b>	<b>15</b>
Considerations	15
Supported FortiClient features	15
Common use cases	19
SIA for FortiClient agent-based remote users	20
SIA for FortiExtender site-based remote users	20
SIA for FortiGate SD-WAN secure edge site-based remote users	21
SIA for FortiAP site-based remote users	22
SIA for SD-WAN On-Ramp site-based remote users	22
Supported SD-WAN On-Ramp IPsec devices	23
Log forwarding	23
Central management using FortiManager	23
RBI	23
ZTNA	24
SPA	24
SPA Service Connection license	24
SPA FortiCloud account prerequisites	24
SPA using a FortiGate SD-WAN hub	25
SPA using a FortiSASE SPA hub	25
SPA using FortiGate SASE bundle license	25
SPA using a FortiSASE SPA hub with Fabric overlay orchestrator	26
SPA for an MSSP hub	27
Data protection using FortiCASB	27

---

<b>Resolved issues</b>	<b>28</b>
<b>Known issues</b>	<b>29</b>
New known issues	29
Existing known issues	29
<b>Limitations</b>	<b>31</b>
FortiAP	31
FortiClient (Android)	31
FortiClient (iOS)	31
FortiClient Cloud	31
FortiCloud	31
FortiClient desktop (Windows, macOS, Linux)	32
FortiSandbox	32
Agentless ZTNA	32
Authentication	33
Security features	33
VPN Policies	33

# Change log

Date	Change description
2025-05-09	Initial release.
2025-05-14	Updated: <ul style="list-style-type: none"><li>• <a href="#">Product integration and support on page 15</a></li><li>• <a href="#">Resolved issues on page 28</a></li><li>• <a href="#">New known issues on page 29</a></li></ul>
2025-05-21	Added <a href="#">What's new for 25.2.24 (25.2.a)</a> on page 7. Updated: <ul style="list-style-type: none"><li>• <a href="#">Resolved issues on page 28</a></li><li>• <a href="#">New known issues on page 29</a></li></ul>
2025-05-22	Updated <a href="#">Product integration and support on page 15</a> .
2025-05-26	Updated <a href="#">Resolved issues on page 28</a> .

# Introduction

This document provides a list of new features and changes and known issues for FortiSASE 25.2.30. Review all sections of this document before using this service.

# What's new

- What's new for 25.2.30 (25.2.a.1) on page 7
- What's new for 25.2.24 (25.2.a) on page 7
- What's new for 25.1.75 (25.1.c) on page 8
- What's new for 25.1.51 (25.1.b) on page 8
- What's new for 25.1.39 (25.1.a.2) on page 9
- What's new for 25.1.37 (25.1.a.1) on page 9
- What's new for 25.1.28 (25.1.a) on page 9

## What's new for 25.2.30 (25.2.a.1)

25.2.a.1 is a maintenance release. For a list of resolved issues, see [Resolved issues on page 28](#).

## What's new for 25.2.24 (25.2.a)

- Added support for FortiGate SASE Bundle license to accelerate the journey from SD-WAN to SASE. The bundle includes a Starter Kit with FortiSASE Standard remote user licenses and Secure Private Access (SPA) connectivity to G-series FortiGate models starting with 120G.
- FortiClient 7.2.9 is the recommended supported version for existing and new FortiSASE instances using IPsec and SSL VPN remote user connectivity. See [Product integration and support on page 15](#).
- Added support to enhance default pre-logon tunnel security settings for IPsec by using stronger hashing algorithm (SHA 256) and key exchange algorithm (DH group 15) with IKE version 2. See [10607](#).
- Access to Fortinet or Regional Public Cloud Locations and features included with the Advanced remote users FortiSASE license are now supported with the Professional remote users FortiSASE license. See [Licensing](#).
  - Network performance of Regional Public Cloud Locations differs from Public Cloud Locations supported with the Comprehensive license.
  - Since dedicated public IPs are provided by the Public Cloud provider, IP reputation control is not guaranteed, and source IP anchoring is not supported.
- Added support for the Global Region Add-on license that can be added on top of an existing Comprehensive license. This add-on license entitles the instance to use an unlimited number of Security PoPs selected from existing and future Fortinet Cloud and Public Cloud locations. See [Appendix A - FortiSASE data centers](#).
- Added support for registering FortiCASB data protection add-on licenses. See [Product integration and support on page 15](#).
- Number of private applications supported per agentless ZTNA bookmark policy increased from 20 to 200. See [Configuring the bookmark portal](#).

## What's new for 25.1.75 (25.1.c)

- Added support for displaying endpoint details in *Network > Managed Endpoints > Endpoints* and *Network > Connected Users* including *FortiSASE VPN Tunnel IP* and *FortiSASE agent session* details, and the *Last Seen* timestamp in *Managed Endpoints*. The *FortiSASE VPN Tunnel IP* can be used with server-client applications with server traffic originating from SPA hubs destined for a FortiSASE managed endpoint. See [Managed Endpoints](#) and [Connected Users](#).
- Added support for displaying the learned BGP multi-exit discriminator (MED) values in *Health and VPN Tunnel Status > View Learned BGP Routes* when *Network > Network Configuration* is configured with *Hub selection method as BGP MED*. See [Viewing MED values of SPA routes](#) and [Viewing health and VPN tunnel status](#).
- Added data center support for Querétaro, Mexico and Sydney, Australia as Public Cloud locations. See [Global data centers](#).
- Added data center support for Sao Paulo, Brazil as a Fortinet Cloud location. See [Global data centers](#).

## What's new for 25.1.51 (25.1.b)

- Added support for the SD-WAN On-Ramp connection add-on license for 1-2000 FortiGate IPsec connections. Since you can purchase a maximum of eight SD-WAN On-Ramp locations for a single account, with SD-WAN On-Ramp connection add-on licenses it is possible for an account to have a maximum of 16000 SD-WAN On-Ramp connections. See [SD-WAN On-Ramp](#).
- Added support for the agentless zero trust network access (ZTNA) bookmark portal to show private applications' bookmarks based on the authenticated user's permission level which is controlled by Agentless ZTNA bookmark policies. See [Configuring the bookmark portal](#).
- Added enhancements to the Network Lockdown feature by enabling FortiClient endpoints to enter strict lockdown with a configurable grace period of 0 seconds. Also added support for detecting and exempting traffic to captive portals and domains specified under *Exempt destinations*. See [Network lockdown](#).
- Added enhancements to the Geofencing feature by enabling granular control over prioritization of connection attempts and failover to connections of type On-premise device and Security PoP based on the endpoint's country or region. See [Geofencing](#).
- Added support for administrators to clone endpoint profiles using an existing endpoint profile, simplifying profile management and reducing configuration time. See [Profiles](#).
- Added support to configuration of ZTNA application gateway and ZTNA destinations under *Configuration > Agent-based ZTNA*. These configuration settings can now be easily referenced and applied to individual endpoint profiles under ZTNA tab, streamlining ZTNA configuration. See [ZTNA](#).
- Added enhancements to Digital Experience Monitoring (DEM), enabling FortiSASE administrators to view TCP latency metrics for endpoints as a Beta feature, offering deeper visibility into underlay network performance from the endpoint to FortiSASE Security PoP. See [Digital experience: TCP latency](#).
- Added support for an increased maximum number of FortiAP edge devices that FortiSASE supports. See [SIA for FortiAP site-based remote users on page 22](#).
- Added datacenter support for Madrid, Spain as a Fortinet Cloud location. See [Global data centers](#).
- Added support for signing a preconfigured FortiClient installer using your own CA certificate or using the Fortinet CA certificate via [FortiCare Support](#) ticket request.



## What's new for 25.1.39 (25.1.a.2)

25.1.a.2 is a maintenance release. For a list of resolved issues, see [Resolved issues on page 28](#).

## What's new for 25.1.37 (25.1.a.1)

25.1.a.1 is a maintenance release. For a list of resolved issues, see [Resolved issues on page 28](#).

## What's new for 25.1.28 (25.1.a)

- Added support in endpoint profiles for enabling patching of vulnerabilities detected where automatic patching is available and for configuring the minimum severity level of vulnerabilities to patch. Also, added support in the *Vulnerability Summary* widget for selecting individual vulnerabilities to schedule to be automatically patched on affected endpoints. See [Drilling down on vulnerabilities](#).
- Added support for configuring schedules and service groups for VPN and secure web gateway (SWG) policies, both Internet Access and Private Access policies. See [Adding policies to perform granular firewall actions and inspection](#).
- Added support for synchronization of service groups for VPN and SWG policies using FortiManager with the central management select availability feature. See [Central Management](#).
- Added support for adding administrator-defined comments to VPN and SWG policies, both Internet Access and Private Access policies. See [Adding policies to perform granular firewall actions and inspection](#).
- Added support to allow administrators to configure, edit, and delete personal VPN settings on FortiClient on per-endpoint profile basis. As FortiSASE does not manage personal VPN settings, enabling this feature is recommended only for endpoint profiles designated for FortiClient users belonging to your organization's administrative group. This ensures flexibility while maintaining security and compliance across managed devices. See [Connection](#).
- Added support to allow remote VPN users to access their local network resources such as printers or fileshares while remaining connected to FortiSASE secure internet access (SIA). You can enable this feature on a per-endpoint profile basis. Additionally, if you enable on-net detection, you can enable the feature based on an endpoint's on-net status, allowing more granularity. See [Connection](#).
- Extended existing REST API support to include security profiles, user groups, and authentication sources.
- Added datacenter support for Plano, Texas, USA as a Fortinet Cloud location. See [Global data centers](#).
- FortiClient 7.2.8 is the recommended supported version for existing and new FortiSASE instances using SSL VPN and IPsec remote user connectivity.
- Added support for displaying comprehensive error messages for failed synchronization attempts when using FortiManager with the central management select availability feature. See [Displaying error messages for failed synchronization attempts](#).
- Added support for authenticating agent-based remote users via SAML single sign on (SSO) during their onboarding. FortiSASE acts as a service provider, supporting integration with other identity providers such as FortiAuthenticator, Okta, and Microsoft Entra ID to ensure that only authenticated users can connect to the FortiSASE Endpoint Management service using an invitation code. This is a select availability feature and you must enable it for it to be visible under *Configuration > User Onboarding SSO*. See [User onboarding SSO](#).

- Added support for administrators to add, change, and delete security PoP locations dynamically from *Network > Infrastructure* as a select availability feature. See [Infrastructure](#). This is available only when a FortiSASE instance meets these specific conditions:
  - The following features are not configured:
    - SWG
    - Source IP address anchoring
  - Default VPN remote users' IP address range has not been exceeded.
  - The following have not been deployed:
    - Edge devices
    - SD-WAN On-Ramp locations
  - Other custom changes to the instance have not been made.

# Special notices

## On-shore Dubai customers

The DXB-F2 Fortinet Cloud datacenter location in Dubai, United Arab Emirates (UAE) uses an on-shore local internet service provider, ensuring compliance with local UAE regulations. To comply with UAE regulations and to avoid latency issues, all on-shore (domestic) customers must use this location. See [Global data centers](#).

## Removable media access

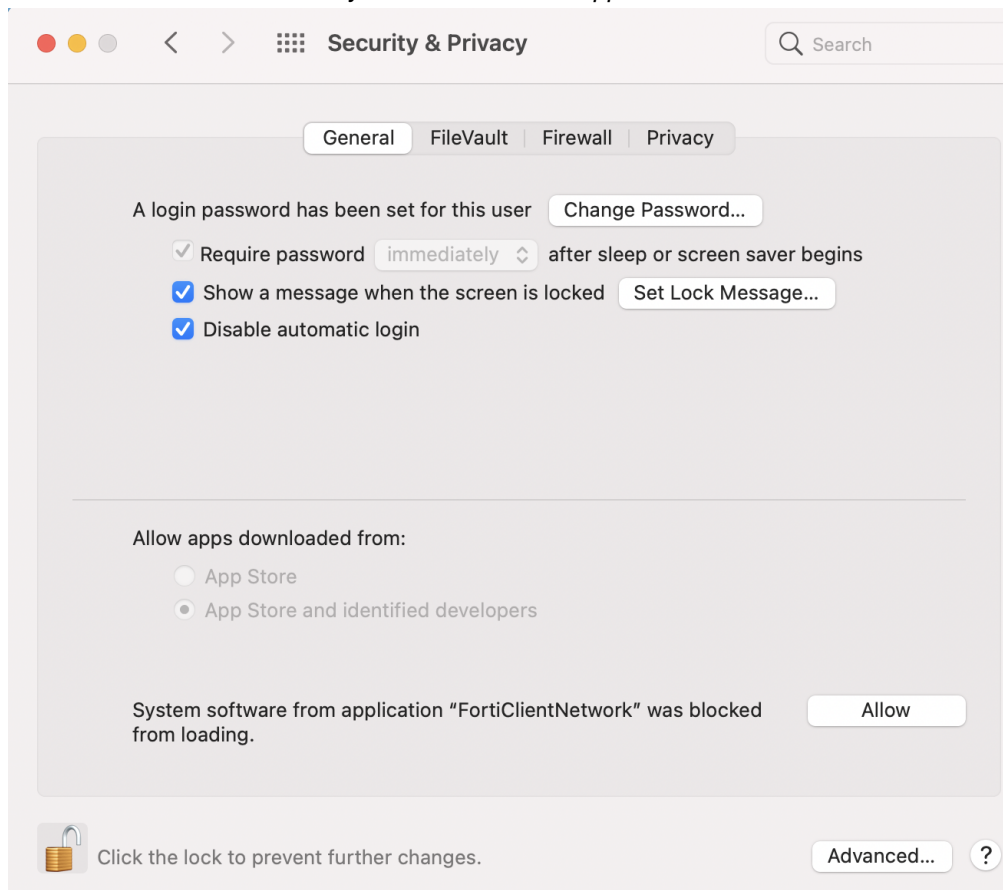
The *Profile > Removable Media Access Control* option only works if you enable Malware Protection, an optional feature, when installing FortiClient on the endpoint.

## Activating the FortiClientNetwork extension

After you connect FortiClient (macOS) to FortiSASE, attempts to connect to SSL VPN may fail unless you enable the FortiClientNetwork extension. The FortiSASE team ID is AH4XFXJ7DK. See the [FortiClient \(macOS\) 7.0.13 Release Notes](#).

**To enable the FortiClientNetwork extension:**

1. Go to *System Preferences > Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.



3. Verify the status of the extension by running the `systemextensionsctl list` command in the macOS terminal. The following provides example output when the extension is enabled:

```
MacBook-Air ~ % systemextensionsctl list
2 extension(s)
-- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * AH4XFXJ7DK com.fortinet.forticlient.macos.vpn.mwextension (1.4.8/B20210629) vpnprovider [activated]
* * AH4XFXJ7DK com.fortinet.forticlient.macos.webfilter (1.1/1) FortiClientPacketFilter [activated enabled]
```

# Select availability features

FortiSASE includes several features with select availability, which are features that are released but are not available by default for all customers. See [Select availability features](#).

# Beta features

Features marked as "Beta" are available to use but may have constraints. These features are subject to continual improvements. Feedback is encouraged. See [Beta features](#).

# Product integration and support

FortiSASE supports the following FortiClient versions:

- [FortiClient \(Windows\) 7.2.9](#)
- [FortiClient \(macOS\) 7.2.9](#)
- [FortiClient \(Linux\) 7.0.13](#)
- [FortiClient \(Android\)](#)
- [FortiClient \(iOS\)](#)

FortiClient 7.2.9 is the recommended version for FortiSASE for desktop users. FortiSASE has updated installers and download links to use FortiClient 7.2.9.

- The "recommended version" is the preferred agent release with full compatibility with FortiSASE features.
- [Fortinet Support](#) supports newer FortiClient versions on a best-effort basis as they are not yet officially recommended versions for FortiSASE. Newer versions are agent releases newer than the recommended version, which resolve known issues for specific customer deployments.
- [Fortinet Support](#) supports older versions until these FortiClient versions are no longer fully supported with FortiSASE. Older versions are earlier agent releases which were previously recommended versions for FortiSASE.
- Newer and older versions pertain to patch releases within the same minor releases. Currently, only patch versions within FortiClient 7.2 are supported for FortiSASE.

## Considerations

- For existing instances created before 24.4.b.1 with remote user connectivity to FortiSASE using SSL VPN, the recommended version is FortiClient 7.2.9.
- Starting in FortiSASE 24.4.b.1, IPsec VPN remote user support is enabled by default on new instances.
  - For instances with IPsec VPN remote user support enabled, the recommended version is FortiClient 7.2.9.
  - For instances created before 24.4.b.1, implementing IPsec VPN remote user support is a significant mode change that impacts the overall FortiSASE instance operation. It has several constraints and is subject to continual improvements.
  - You cannot disable or revert IPsec VPN remote user support implementation without significant data loss and service disruption.
  - Fortinet recommends that you only raise a request to implement IPsec VPN remote user support after careful consideration and understanding of impact and service disruptions.

## Supported FortiClient features

The following table lists the FortiClient platform and version and each version's corresponding features that FortiSASE supports:

Feature	Windows 7.2.9	macOS 7.2.9	Linux 7.0.13	Android	iOS
Diagnostic logs on-demand requests from FortiSASE	✓				
Digital experience monitoring agent*	✓	✓			
FortiGuard Forensics Analysis*	✓				
<b>Access</b>					
Autoconnect to FortiSASE using Microsoft Entra ID credentials	✓				
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓	✓		✓	✓
Bypass FortiSASE using application-based split tunnel	✓				
Bypass FortiSASE using on-net endpoint detection via DNS server	✓	✓	✓		
Bypass FortiSASE using on-net endpoint detection via DHCP server	✓	✓	✓		
Bypass FortiSASE using on-net endpoint detection via local subnet	✓	✓	✓		
Bypass FortiSASE using on-net endpoint detection via ping server	✓	✓	✓		
Bypass FortiSASE using on-net endpoint detection	✓	✓	✓		



Feature	Windows 7.2.9	macOS 7.2.9	Linux 7.0.13	Android	iOS
via public IP address					
Endpoint profile assignment based on Microsoft Entra ID groups	✓				
Endpoint profile change notifications	✓	✓	✓		
Endpoint telemetry	✓	✓	✓	✓	✓
Endpoint VPN connectivity notifications	✓	✓	✓		
Endpoint VPN disconnection by disabling management connection from FortiSASE	✓	✓	✓		
External browser as user-agent for SAML login			✓		
Force always on VPN	✓	✓	✓	✓	✓ FortiClient (iOS) does not disable the VPN button instantly. You must navigate away from the VPN page to disable the VPN button.
IPsec VPN to FortiSASE	✓	✓			
Network lockdown	✓	✓			
Pre-logon VPN	✓				

Feature	Windows 7.2.9	macOS 7.2.9	Linux 7.0.13	Android	iOS
Show zero trust network access (ZTNA) tags on FortiClient	✓	✓	✓		✓ Does not support hiding tags.
Split DNS	✓	✓			
SSL VPN connection remains active after endpoint has been idle	✓	✓	✓		✓
SSL VPN support for DTLS**	✓	✓			
SSL VPN to FortiSASE			✓	✓	✓
<b>FSSO</b>					
FortiClient SSO mobility agent	✓	✓			
<b>Protection</b>					
Antiransomware	✓				
Next generation antivirus (AV) – real-time AV and cloud malware protection	✓	✓	✓		
Removable media access control	✓	✓ FortiClient (macOS) does not support rules. It only supports allow and block actions.	✓ FortiClient (Linux) does not support rules. It only supports allow and block actions.		
Removable media access control – notify endpoint of blocks		✓	✓		

Feature	Windows 7.2.9	macOS 7.2.9	Linux 7.0.13	Android	iOS
Vulnerability scan	✓	✓	✓		
Vulnerability scan - event-based scan	✓	✓	✓		
<b>Sandbox</b>					
Sandboxing - on-premise and FortiSASE Cloud Sandbox	✓	✓			
<b>ZTNA</b>					
ZTNA remote access	✓	✓	✓		
ZTNA tagging rules	✓	✓	✓	✓	✓

\* Requires Advanced or Comprehensive License

\*\* DTLS support is enabled by default for existing and new FortiSASE instances.

## Common use cases

To connect to a FortiSandbox appliance behind a firewall, you must open ports 514 and 443.

In some scenarios, FortiSASE interacts with other Fortinet products. The following lists the supported versions for each scenario:

Use case	Description
<a href="#">SIA for FortiClient agent-based remote users on page 20</a>	Secure access to the internet using FortiClient agent.
<a href="#">SIA for FortiExtender site-based remote users on page 20</a>	Secure access to the internet using Thin Edge FortiExtender device as FortiSASE LAN extension.
<a href="#">SIA for FortiGate SD-WAN secure edge site-based remote users on page 21</a>	Secure access to the internet using FortiGate SD-WAN Secure Edge device as FortiSASE LAN extension.
<a href="#">SIA for FortiAP site-based remote users on page 22</a>	Secure access to the internet using FortiAP device as FortiSASE edge device.
<a href="#">SIA for SD-WAN On-Ramp site-based remote users on page 22</a>	Secure access to the internet using SD-WAN devices via IPsec acting as an on-ramp to FortiSASE.

Use case	Description
<a href="#">Log forwarding on page 23</a>	Forward logs to an external server, such as FortiAnalyzer.
<a href="#">Central management using FortiManager on page 23</a>	Centrally manage FortiSASE configuration settings from FortiManager
<a href="#">RBI on page 23</a>	For secure web gateway (SWG) users, isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container.
<a href="#">ZTNA on page 24</a>	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases.
<a href="#">SPA using a FortiGate SD-WAN hub on page 25</a>	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network.
<a href="#">SPA using a FortiSASE SPA hub on page 25</a>	Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW).
<a href="#">SPA using FortiGate SASE bundle license on page 25</a>	Seamless integration of FortiGate with FortiSASE for SPA to simplify the journey from SD-WAN to SASE.
<a href="#">SPA using a FortiSASE SPA hub with Fabric overlay orchestrator on page 26</a>	Access to private company-hosted applications behind the FortiGate NGFW using Fabric Overlay Orchestrator.
<a href="#">SPA for an MSSP hub on page 27</a>	Access to private company-hosted applications behind the FortiGate secure private access (SPA) hub shared in a managed security service provider (MSSP), multi-tenant environment.
<a href="#">Data protection using FortiCASB on page 27</a>	Visibility, compliance, data security, and threat protection for cloud-based services.

## SIA for FortiClient agent-based remote users

To allow remote users to connect to FortiSASE, ensure you have purchased the per-user FortiSASE licensing contracts and applied them to FortiCloud.

See the [supported FortiClient versions](#).

## SIA for FortiExtender site-based remote users

FortiSASE supports FortiExtender models for the LAN extension feature. The FortiExtender should run 7.4.3 and later. This feature requires a separate FortiSASE subscription license per FortiExtender.

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.

FortiSASE supports a maximum of 1024 FortiExtender devices combined that you can configure as FortiSASE edge devices.

Certain FortiExtender models are equipped with wired and/or wireless capabilities, along with advanced performance metrics to extend your microbranch LAN deployments. These models, also known as FortiBranchSASE, provide superior performance and flexibility.

The following table lists key features for different FortiExtender models that the FortiSASE for LAN extension feature supports:

Feature	FortiExtender 200F	FortiBranchSASE 20G	FortiBranchSASE 20G WiFi	FortiBranchSASE 10F WiFi
LAN extension	✓	✓	✓	✓
Zero-touch provisioning	✓	✓	✓	✓
Wi-Fi support			✓	✓
Ethernet support	✓	✓	✓	✓
Available Ethernet ports	5 x GbE RJ45	4 x 1GE RJ45 + 1 SFP/RJ45	4 x 1GE RJ45 + 1 SFP/RJ45	2 x 1GE RJ45

For information on FortiBranchSASE, see the [FortiBranchSASE series datasheet](#).



For existing instances provisioned before FortiSASE 24.1.b and using FortiExtender, create a new FortiCare ticket to have the resolution for the resolved issue in Bug ID 1003287 applied to your instance. See [Resolved issues on page 28](#) for relevant issues resolved.

## SIA for FortiGate SD-WAN secure edge site-based remote users

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

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.

FortiSASE supports a maximum of 16 FortiGate and FortiWiFi devices combined that you can configure as FortiSASE edge devices.

## SIA for FortiAP site-based remote users

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

- FortiAP 23JF, 231F, 234F, 431F, 432F, 432FR, 433F, 831F
- FortiAP 231G, 233G, 234G, 431G, 432G, 433G

FortiSASE also supports profile configuration for 6G connectivity and LAN port management for selected FortiAP models.

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

FortiSASE supports a maximum of 240 FortiAP devices that you can configure as FortiSASE edge devices.

## SIA for SD-WAN On-Ramp site-based remote users

FortiSASE SD-WAN On-Ramp enables customers to connect certified IPsec devices for inbound connectivity to FortiSASE for secure internet access (SIA), secure SaaS access, and SPA. IPsec service connections require the FortiSASE instance to have these licenses applied:

- Advanced or Comprehensive license
- FortiSASE SD-WAN On-Ramp Location subscription license corresponding to the Advanced or Comprehensive license

See the [FortiSASE Ordering Guide](#).



SD-WAN On-Ramp and SPA share BGP configuration. You must configure the SPA network configuration before deploying an SD-WAN On-Ramp location but you can create SPA service connections after deploying an SD-WAN On-Ramp location.

---

The FortiSASE SD-WAN On-Ramp Location subscription license has these features:

- IPsec connectivity to a number of FortiSASE locations depending on the number of connections (two to eight) that the license specifies
- 1 Gbps of shared bandwidth for up to 10 simultaneous dialup IPsec connections from the IPsec device to the selected FortiSASE locations
- FQDN and static IP address to use for each IPsec On-Ramp location
- Enable connectivity from different IPsec device types as part of the same license

You must purchase the license multiple times if the expected bandwidth exceeds 1 Gbps for the location or the number of connected devices in one location exceeds 10.

Alternatively, if you require more than 10 connected devices in one location, you can purchase the SD-WAN On-Ramp Connection add-on license corresponding to the Advanced or Comprehensive license. This add-on can be purchased in increments of 1-2000 per location. With a maximum of 8 locations for on-ramp connections and maximum of 2000 connections per location, customers can have up to 16000 connections per account.

For example, if a customer has 200 branches using SD-WAN On-Ramp then 200 connections are required, and the following licenses can be purchased:

- 2 SD-WAN On-Ramp Location licenses, each including 10 connections for a total of 20 connections
- 1 SD-WAN On-Ramp Connection add-on license containing 180 connections:
  - Assign 90 connections to first On-Ramp location
  - Assign 90 connections to second On-Ramp location

See the [FortiSASE Ordering Guide](#).

## Supported SD-WAN On-Ramp IPsec devices

Device	Supported firmware version
FortiGate	7.2.8 or later

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

## Log forwarding

If using FortiAnalyzer for log forwarding, the FortiAnalyzer should be on 7.0.4 or later.

## Central management using FortiManager

When using FortiManager for central management, the FortiManager or FortiManager Cloud should be on 7.4.4 or a later 7.4 version and only FortiManager VM platforms are supported. FortiSASE does not support using FortiManager 7.6 or FortiManager Cloud 7.6 for central management.

- You cannot add FortiSASE to version 7.0 administrative domains (ADOM) or the global ADOM.
- FortiManager only supports adding FortiSASE to FortiGate and Fabric ADOMs. Other ADOMs where the connector appears including FortiProxy, FortiFirewallCarrier, FortiFirewall, FortiCarrier, and the Global Database ADOMs are not supported. Additionally, you cannot add FortiSASE to ADOMs operating in backup mode. Attempting to do so presents the user with an *An unexpected error has occurred* error.

## RBI

FortiSASE must have an Advanced remote users license to use remote browser isolation (RBI) with the following limitations:

- Supported for SWG users only
- Maximum of five simultaneous RBI sessions per user
- Sessions time out after 10 minutes of inactivity
- 100 MB of monthly isolation data per user included (1.2 GB per year)

## ZTNA

If using ZTNA, the FortiGate acting as the ZTNA access proxy should be on the following FortiOS versions:

- 7.0.10 or later
- 7.2.4 or later

## SPA

For securing private TCP- and UDP-based applications, FortiSASE supports a SPA deployment using an existing FortiGate SD-WAN hub or SPA using a FortiGate NGFW converted to a standalone FortiSASE SPA hub. These SPA use cases are based on IPsec VPN overlays and BGP.

## SPA Service Connection license

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 NGFW location only.
- FortiGate 100F series and later are recommended for an SD-WAN hub.

See the [FortiSASE Ordering Guide](#).

For the MSSP hub use case, see [SPA for an MSSP hub on page 27](#).

## SPA FortiCloud account prerequisites

You must register FortiGate devices to the same FortiCloud account used to log into FortiSASE before using these devices as SPA hubs with FortiSASE.

To activate the SPA feature on FortiSASE, you must purchase and apply a FortiSASE Service Connection license to each FortiGate device registered.

For details on registering products, see [Registering assets](#).



## SPA using a FortiGate SD-WAN hub

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See [SPA Service Connection license](#) and [SPA FortiCloud account prerequisites on page 24](#).

If you deploy SPA using a FortiGate SD-WAN hub, use the following versions:

Product	Supported firmware version
FortiGate	<ul style="list-style-type: none"><li>7.0.10 or later</li><li>7.2.4 or later</li><li>7.4.0 or later</li><li>7.6.0 or later</li></ul>
FortiManager	<ul style="list-style-type: none"><li>7.2.0 or later, which supports SD-WAN overlay templates</li><li>7.0.3 or later, which includes BGP and IPsec VPN recommended templates for SD-WAN overlays</li><li>7.4.0 or later</li></ul>
FortiClient	7.2.9

## SPA using a FortiSASE SPA hub

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See [SPA Service Connection license](#) and [SPA FortiCloud account prerequisites on page 24](#).

If you deploy SPA using a FortiSASE SPA hub, use the following versions:

Product	Supported firmware version
FortiGate	<ul style="list-style-type: none"><li>7.0.10 or later</li><li>7.2.4 or later</li><li>7.4.0 or later</li><li>7.6.0 or later</li></ul>
FortiClient	7.2.9

## SPA using FortiGate SASE bundle license

Fortinet's FortiGate SASE bundle license enables seamless integration of FortiGate with FortiSASE for SPA to simplify the journey from SD-WAN to SASE.

The FortiGate SASE Bundle license is available for FortiGate G-series hardware models starting from 120G and above. Each FortiGate device intended for SPA connectivity must be licensed individually with its own FortiGate SASE SPA Bundle license.

The FortiGate SASE Bundle includes the following:

- FortiSASE SPA: enables SPA connectivity from FortiGate to FortiSASE.
- FortiSASE Standard Starter Kit: includes FortiSASE Standard remote user licenses. The number of included remote user seats depends on the model of G-series FortiGate licensed, outlined as follows:

Model	Included remote user seats for each model
Below 120G	None
120G to 600G	10
900G to 1500G	50
1800G+	100
VM and Cloud	None

The number of remote user seats are cumulative and based on the number and model of FortiGates that have the FortiGate SASE bundle license applied under the same FortiCloud account as FortiSASE. For example, consider that a customer purchases the FortiGate SASE bundle license for:

Device	Included remote user seats for each model
One 120G FortiGate	10
One 900G FortiGate	50

In this case, the total number of included FortiSASE Standard remote user seats is 60 seats (10 + 50).

See the [FortiSASE Ordering Guide](#).

## SPA using a FortiSASE SPA hub with Fabric overlay orchestrator

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See [SPA Service Connection license](#) and [SPA FortiCloud account prerequisites on page 24](#).

If you deploy SPA using a FortiSASE SPA hub with the Fabric Overlay Orchestrator, use the following versions:

Product	Supported firmware version
FortiGate	<ul style="list-style-type: none"> <li>• 7.2.4 or later</li> <li>• 7.4.0 or later</li> <li>• 7.6.0 or later</li> </ul>
FortiClient	7.2.9

The SPA easy configuration key for FortiSASE is supported in the Fabric Overlay Orchestrator in the following FortiOS version:

Product	Supported firmware version
FortiGate	<ul style="list-style-type: none"> <li>• 7.4.5 and later</li> <li>• 7.6.0 and later</li> </ul>

## SPA for an MSSP hub

For MSSPs using FortiCloud Organizations to arrange accounts into a root organizational unit (OU) and sub-OUTs and where many tenants share a FortiGate SPA hub, FortiSASE supports tenants within a sub-OU inheriting SPA licenses from the root OU account.

For a FortiSASE instance within a sub-OU, the number of supported SPA hubs is the sum of the number of SPA licenses registered in the tenant sub-OU account and the number of SPA licenses registered in the root OU, up to a maximum of 12 SPA licenses in total.

## Data protection using FortiCASB

FortiCASB is Fortinet's cloud-native cloud access security broker (CASB) service, which provides visibility, compliance, data security, and threat protection for cloud-based services. FortiSASE supports registering a FortiCASB data protection add-on license. The add-on license must be registered in the same FortiCloud account as FortiSASE. FortiSASE supports FortiCASB 24.4.b.

# Resolved issues

The following issues have been fixed in version 25.2.30. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
1096330	After configuring 1024 FortiExtender devices in FortiSASE, instance encounters resource usage issues.
1140284	Thin Edge device does not get IP address after being reauthorized.
1145052	FortiSASE does not save Implicit-all DNS rule - Private type custom DNS with public IP address with correct configuration, causing DNS resolution issue.
1148373	FortiSASE fails to create policies when central management is enabled.
1155004	Advanced not for resale license: advanced features like digital experience monitoring, forensics analysis, and agentless zero trust network access are not visible on the GUI.
1158147	You cannot upgrade an instance with the FortiSASE secure private access bundle license to the Standard, Professional, Advanced, or Comprehensive license.

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 29](#)
- [Existing known issues on page 29](#)

For inquiries about a particular bug, contact [Customer Service & Support](#).

## New known issues

The following issues have been identified in version 25.2.30. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
1154427	SD-WAN On-Ramp contract cannot be applied on top of FortiSASE Professional license.
1156096	VPN Implicit DNS Rule displayed in GUI for IPSec VPN FortiSASE instance.

## Existing known issues

The following issues were identified in a previous version and remain in 25.2.30. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
716833	FortiClient (macOS) does not support application-based split tunnel.
746224	Clicking <i>Deauthenticate</i> for a secure web gateway (SWG) user in <i>Session Monitor</i> does not deauthenticate the user.
775860	When installing FortiClient on Windows, user may see a warning about FortiClient originating from an unknown publisher if Windows Defender is enabled.
907570	FortiSASE does not support option to test SWG single sign on SAML connectivity.
914278	<i>Managed Endpoints</i> incorrectly displays warning for FortiClient version mismatch for iOS and Android devices.
961542	When enabling Sandbox in an endpoint profile, FortiSASE-managed endpoint running FortiClient (macOS) and Microsoft Defender conflict due to the system processes used in overlapping real time protection features.

Bug ID	Description
	<b>Workaround:</b> enable passive mode on Microsoft Defender.
1039399	Sometimes FortiClient event logs do not upload to FortiSASE. <b>Workaround:</b> contact <a href="#">FortiCare Support</a> to open a ticket to apply a known workaround to your instance.
1067774	User cannot disable FQDN and DNS feeds used in custom security profiles.
1088596	<i>Top WiFi Clients by Bytes</i> may not show all connected devices and may show duplicate devices on <i>FortiView WiFi clients</i> widget.
1098950	Traffic may not reach endpoint when using SAML identity provider authentication in captive portal for FortiExtender devices on some license types.
1109272	Log forwarding from on-prem log server may not be able to reach FortiSASE FortiAnalyzer due to missing default route <b>Workaround:</b> Contact <a href="#">FortiCare Support</a> to open a ticket to apply a known workaround to your instance.
1117848	Unable to download large Diagnostic Logs through Managed Endpoints section of the GUI.
1121555	Cannot configure local IP address 10.255.1.1 as BGP Peer IP on a private access connection.
1122595	Agentless ZTNA private application/bookmark access fails to work as expected intermittently for instances where the number of entitled PoPS exceeds 16 and/or if any entitled PoPs have been provisioned to exceed the default maximum number of VPN remote users per region of 4096 (/20)
1128499	Digital experience monitoring (DEM) on previously connected Windows endpoint does not work after FortiSASE instance is reprovisioned. <b>Workaround:</b> reinstall FortiClient and the DEM agent together on the Windows endpoint.
1131881	Sandbox exclusion regex is not supported in FortiSASE GUI for network mapped drive folder
1143608	FortiSASE Onboarding users email for Manual Installer type have the links for Pre-configured type installers instead.
1155528	Local users are not matched in created policies and are only matched if they are in a local group. <b>Workaround:</b> create a local group with just the local user and specify that group in policies.

# Limitations

## FortiAP

FortiSASE does not recommend firmware versions for FortiAP G-series edge devices and does not indicate whether the installed FortiAP OS version for these devices is up to date.

## FortiClient (Android)

When the CA certificate is downloaded from FortiSASE and manually installed on certain Android devices, untrusted certificate warnings for this certificate display constantly. This behavior is the result of Android system limitations on certain devices.

## FortiClient (iOS)

If *Settings > Apps > Safari > Privacy & Security > Not Secure Connection Warning* is enabled, VPN connection may fail.

## FortiClient Cloud

The FortiSASE license includes the FortiClient Cloud instance that licenses and provisions endpoints. You cannot access the FortiClient Cloud instance to configure it. You must use FortiSASE with the included FortiClient Cloud instance. You cannot apply a FortiSASE license to an existing FortiClient Cloud instance.

## FortiCloud

Support for FortiCloud subuser accounts or subaccounts is discontinued. Therefore, you must use Identity & Access Management (IAM) users in cases where multiple users access the FortiSASE customer portal.

To migrate existing subuser accounts from FortiCloud and convert them to IAM users, see [Migrating sub users](#).

## FortiClient desktop (Windows, macOS, Linux)

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- For an endpoint to be able to connect to FortiSASE via an SSL VPN tunnel, the FortiSASE environment must have at least one SSL VPN allow policy configured. See [Adding policies to perform granular firewall actions and inspection](#).
- Only Windows endpoints running FortiClient 7.0.13 or later support Microsoft Entra ID domains.
- The endpoint upgrade rule does not apply to Entra ID user groups if the FortiClient version on endpoints is 7.0.12 or earlier.
- On FortiClient (macOS), if the *Non-Secure site connections > Warn before connecting to a website over HTTP* option is enabled in Safari and using an external browser for SAML authentication is configured in FortiSASE, VPN connection may fail.



Using alternate VPN clients in combination with FortiSASE is not recommended nor supported.

---

## FortiSandbox

To connect to a FortiSandbox appliance behind a firewall, you must open ports 514 and 443.

## Agentless ZTNA

Although you must configure secure web gateway (SWG) and SWG single sign on (SSO) to configure agentless zero trust network access (ZTNA), you do not need to configure the remote user endpoints for SWG. In other words, you do not need to configure remote user endpoints with a proxy autoconfiguration file or with a CA certificate for SSL deep inspection. Agentless ZTNA simply uses configuration from SWG and SWG SSO for remote user authentication.

When you enable a valid VPN or SWG configuration on a FortiSASE instance, an endpoint enabled with matching VPN or SWG remote user settings cannot access a private application using its agentless ZTNA URL bookmark in the secure application bookmark portal. Agentless ZTNA traffic is proxied to the private application server directly, bypassing the typical secure internet access VPN or SWG traffic flow. This aligns with the agentless ZTNA use case where the user accesses a private application without connecting to FortiSASE as a VPN or SWG user. Therefore, for valid VPN or SWG endpoints, configuring and accessing private applications using secure private access only instead of using agentless ZTNA is best practice.



## Authentication

- Other user authentication methods do not work once you enable SAML SSO.
- Not all options for LDAP server configuration are available on FortiSASE.
- Deauthenticating a SWG SSO user does not direct user to reauthenticate on device without clearing browser cache first.
- For SWG SSO users, to properly proxy legacy Skype traffic, bypass SSO authentication by customizing the PAC file. See [Customizing the PAC file](#).
- For SWG SSO users, at least one SWG policy using SSO authentication must have deep inspection enabled in the configured security profile group. SSO authentication requires deep inspection to work.
  - Any traffic from SWG SSO users that is destined for hosts or URL categories defined as deep inspection exemptions does not work.
  - You must not configure SWG policies using SSO authentication with certificate inspection.
  - If certificate inspection is required in a SWG policy, then SSO authentication must not be configured in that policy.
- LDAP authentication is unavailable for remote VPN users using IPsec VPN.  
**Workaround:** using FortiAuthenticator, configure a RADIUS server that uses remote LDAP server as user repository and configure RADIUS server for remote user authentication in FortiSASE.

## Security features

When Application Control With Inline-CASB and deep inspection are enabled in a security profile group, a replacement message is not provided to the endpoint when traffic is blocked.

## VPN Policies

For SSL VPN remote users, whenever changes are made to an existing Internet Access or Private Access policy, they take effect only after SSL VPN users reconnect to FortiSASE.



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

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.