Release Notes

FortiSASE 25.3.175 Mature

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

February 17, 2026
FortiSASE 25.3.175 Mature Release Notes
72-253175M-1181689-20260217

TABLE OF CONTENTS

Change log

Date	Change description
2026-01-26	Initial release.
2026-01-27	Updated: • What's new on page 7
2026-01-29	Updated: • Product integration and support on page 19
2026-02-02	Updated: • Product integration and support on page 19 Added: • Supported FortiClient features on page 20 • Common use cases on page 28 • Language support on page 35
2026-02-09	Updated: • Common use cases on page 28
2026-02-11	Initial release of 25.4.c.1.
2026-02-12	Updated: • What's new on page 7 • Resolved issues on page 36
2026-02-13	Updated: • What's new on page 7
2026-02-17	Updated: • Resolved issues on page 36

Introduction

This document provides a list of new features and changes and known issues for FortiSASE 25.3.175 Mature. Review all sections of this document before using this service.

What's new

*Infrastructure change only

What's new for 25.3.175 (25.4.c.1 Mature)

There are no changes for 25.4.c.1.

What's new for 25.3.175 (25.4.c Mature)

- Support has been added for FortiClient 7.2.13 for FortiSASE desktop users. This support will be made available some time after the release and is being incrementally deployed for certain tenants. See Product integration and support on page 19.
- Added support for Public Cloud security PoPs: Columbus - Ohio - USA, Montreal - Canada, Moncks Corner - South Carolina - USA, Tokyo - Japan. See Global data centers.

What's new for 25.3.168 (25.4.b.2 Mature)

There are no changes for 25.4.b.2.

What's new for 25.3.168 (25.4.b.1 Mature)

25.4.b.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.168 (25.4.b Mature)

- Added the *Disable native Windows captive portal prompt* option, which when enabled means that FortiClient will handle the captive portal on Windows endpoints.
  - This option is only available when *Lockdown endpoint when off-net* (network lockdown) is enabled.
  - The default setting for this option is disabled, which means that Windows handles the captive portal on endpoints. This ensures that when network lockdown is enabled, WiFi does not disconnect after agent tunnel disconnects.

  See Network lockdown.
- Added support for Public Cloud security PoPs: Frankfurt - Germany, Paris - France, Singapore - Republic of Singapore, Toronto - Canada. See Global data centers.
- Updated support for Fortinet security PoPs: Ashburn - Virginia - USA. See Global data centers.

What's new for 25.3.148 (25.4.a Mature)

- Enhanced ZTNA tag validation for VPN policy enforcement to improve VPN tunnel connectivity and to improve reliability in cases when FortiSASE Endpoint Management service is unavailable. See Tagging.
- Added support for Public Cloud security PoPs: London - United Kingdom, St. Ghislain - Belgium, Warsaw - Poland, Zurich - Switzerland. See Global data centers.

What's new for 25.3.148 (25.3.c.1 Mature)

25.3.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.134 Mature (25.3.c Mature)

- Support FortiClient 7.2.12 as the recommended version for FortiSASE desktop users. See Product integration and support on page 19.

- The UI version has been removed from the FortiSASE portal URL, ensuring a consistent path for ease of access.
- Added support for Delhi, India as a Public Cloud security PoP. See Global data centers.

What's new for 25.3.112 Mature (25.3.b.1 Mature)

25.3.b.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.89 Mature (25.3.b Mature)

- Added Feature or Mature tag to the version tooltip at the bottom of the navigation menu. See New major features available.
- Added support for highlighting best practices recommendations by displaying an additional prompt upon portal login. **For the Mature release, the *New major features available* best practice has been highlighted**.
- Added support for branch on-ramp with the Standard subscription **after applying the *New major features available* best practice to upgrade an existing instance**. An Advanced branch on-ramp subscription must also be applied to a Standard instance to enable the branch on-ramp feature. See SIA for Branch On-ramp site-based remote users.
- Added support for simplified branch on-ramp licensing. See SIA for Branch On-ramp site-based remote users.
  - Each on-ramp Security PoP provides up to 1 Gbps for up to 2000 simultaneous dialup IPsec connections, changed from the previous limit of 10 connections, and includes 50 TB of data transfer per year based on 50 Mbps usage during business hours.
  - Data transfer is aggregated at the account level and shared with remote users (250 GB per user).
  - Additional data transfer subscriptions can be purchased if required.
  - The Branch On-ramp Connection add-on subscription is discontinued after this release. See SIA for Branch On-ramp site-based remote users.

What's new for 25.3.67 Mature (25.3.a.3 Mature)

25.3.a.3 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.57 Mature (25.3.a.2 Mature)

25.3.a.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.47 Mature (25.3.a.1 Mature)

25.3.a.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.3.40 Mature (25.3.a Mature)

- Added support for customizing captive portal replacement message for Edge devices. See HTML templates.
- Added support for customers having Advanced remote user subscriptions to select certain Public cloud locations to launch their FortiSASE Security PoPs. See Global data centers.
- Support FortiClient 7.2.11 as the recommended version for FortiSASE desktop users. See Product integration and support on page 19.
- Added support for Dublin, Ireland (DUB-A2) as a Public Cloud security PoP. Contact FortiCare Support to upgrade to FortiSASE Feature in order to support provisioning of this Security PoP. See Global data centers.

What's new for 25.2.91 Mature (25.2.c.2 Mature)

25.2.c.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.2.90 Mature (25.2.c.1 Mature)

25.2.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.2.81 Mature (25.2.c Mature)

- Support FortiClient 7.2.10 as the recommended version for FortiSASE desktop users. See Product integration and support on page 19.
- Added a new audit page providing configuration best practice recommendations. See Software audit & version.
- Option to upgrade to new major features from the audit page that appears once available for your tenant. This upgrade option is being incrementally deployed. See New major features available.
- Once the new major features upgrade option is available for your tenant and is visible in the audit page, as part of this upgrade option, if your tenant is using the Standard subscription, it will be upgraded to support

dedicated public IP addresses without additional licensing. See New major features available.

- Using the single upgrade option from the audit page offers access to new major features for enhanced FortiSASE functionality. **These features are not available if you do not use the upgrade option.** See the following for examples of these new features. For the complete list, see New features.
  - Navigation menu items have been reorganized for improved usability and to group items with related functionality and usage. Terminology has been standardized for clarity and consistency.
  - Added *System > License overview* page to provide FortiSASE licensing details.
  - Integrated FortiCASB API-based cloud access security broker (CASB) management and protection into FortiSASE for secure SaaS access (SSA).
  - Added DLP enhancements including support for DLP Exact Data Matching (EDM) and Indexed Document Matching (IDM) with DLP fingerprinting.
  - Support IPsec connections to Branch On-ramp Security PoPs from third-party IPsec devices.
  - DNS redirection (formerly split DNS) rules transparently apply to all passthrough traffic for FortiClient agent tunnels, Edge device clients, and Proxy clients.

What's new for 25.2.56 (25.2.b.2)

25.2.b.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.2.48 (25.2.b.1)

25.2.b.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 36.

What's new for 25.2.45 (25.2.b)

- FortiSASE now supports Branch On-ramp deployment for up to 20 On-Ramp locations.
- Improved site provisioning process for new tenant with additional recovery mechanism when a site provision does not complete successfully. See PoPs.

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 36.

What's new for 25.2.24 (25.2.a)

- Added support for FortiGate SASE Bundle subscription to accelerate the journey from SD-WAN to SASE. The bundle includes a Starter Kit with FortiSASE Standard remote user subscriptions 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 19.
- 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.
- Added support for the Global Region Add-on subscription that can be added on top of an existing Comprehensive subscription. This add-on subscription 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 subscriptions. See Product integration and support on page 19.
- 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 Branch On-ramp connection add-on subscription for 1-2000 FortiGate IPsec connections. Since you can purchase a maximum of eight Branch On-ramp locations for a single account, with Branch On-ramp connection add-on subscriptions it is possible for an account to have a maximum of 16000 Branch 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 Product integration and support on page 19.
- 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 36.

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 36.

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 allows 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
    - Branch 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

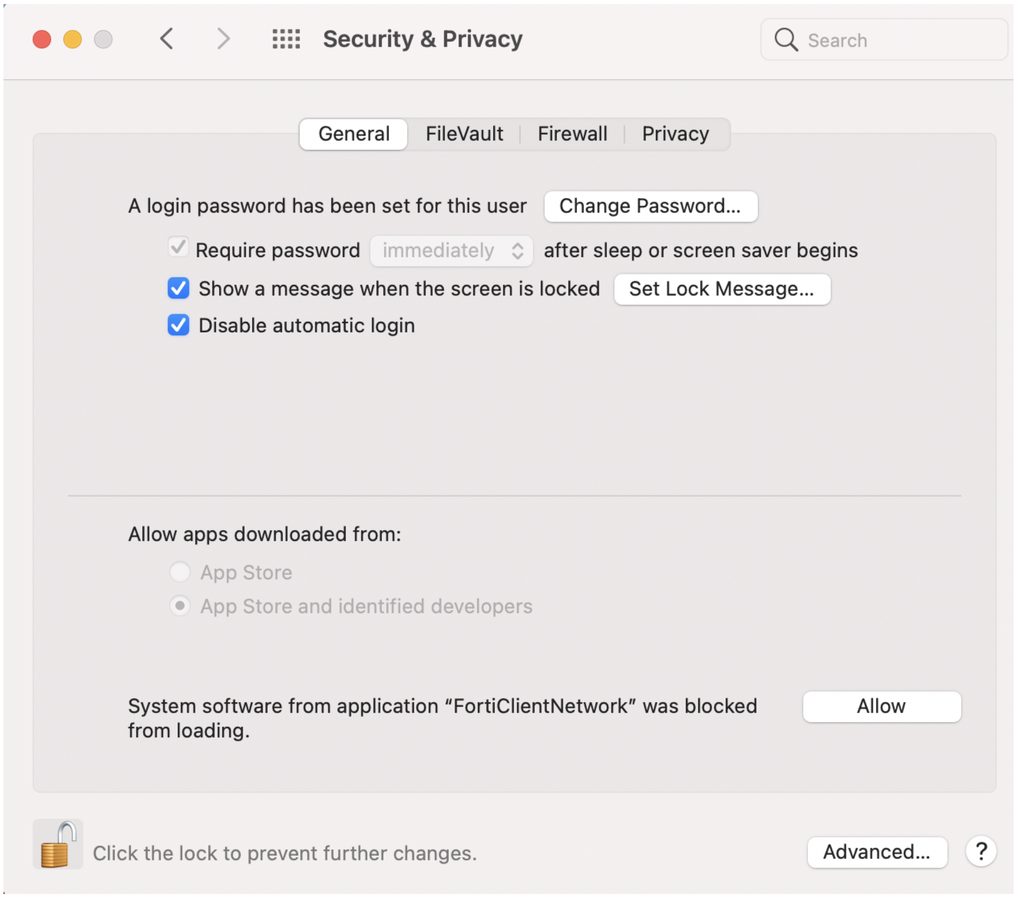
The *Profile > Removable Media Access Control* option only works if you enable Malware Protection, an optional feature, when installing FortiClient on the endpoint.

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*.



Security & Privacy

A login password has been set for this user

☑ Require password immediately after sleep or screen saver begins

☑ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

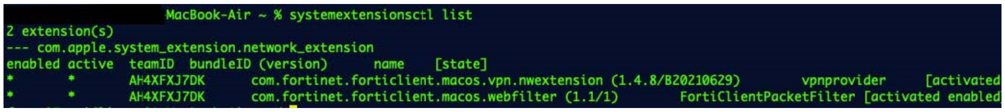
○ App Store

● App Store and identified developers

System software from application “FortiClientNetwork” was blocked from loading.

Click the lock to prevent further changes.

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:



```
[redacted] 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.nwextension (1.4.8/B20210629)        vpnprovider     [activated
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.1/1)        FortiClientPacketFilter [activated enabled
```

Entra ID integration support limitation

FortiSASE supports Entra ID integration with Azure commercial subscription only. Azure Government (e.g. GCC, GCC High, GCC DoD) is not supported.

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) 7.2.13
- FortiClient (macOS) 7.2.13
- FortiClient (Linux) 7.0.13
- FortiClient (Android)
- FortiClient (iOS)

FortiClient 7.2.13 is the recommended version for FortiSASE for desktop users. FortiSASE has updated installers and download links to use FortiClient 7.2.13.

- 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. 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 7.2.13.
- 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 7.2.13.
  - 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.

This section includes the following information:

Supported FortiClient features

IPsec VPN remote user connectivity

The following table lists the FortiClient platform and version and each version's corresponding features that FortiSASE supports for IPsec VPN remote user connectivity:

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
Diagnostic logs on-demand requests from FortiSASE	✓				
Digital experience monitoring agent*	✓	✓			
FortiGuard Forensics Analysis*	✓				
Access					
Autoconnect to FortiSASE using Microsoft Entra ID credentials					
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓	✓		✓	✓
Bypass FortiSASE using application-based split tunnel	✓				
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via DNS server	✓	✓	✓		
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via DHCP server	✓	✓	✓		
Exempt endpoint	✓	✓	✓		

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
from FortiSASE autoconnect when endpoint is on-net via local subnet					
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via ping server	✓	✓	✓		
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net 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	✓	✓	✓	✓	✓

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
					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 using IKEv2, Preshared Key, and SAML	✓	✓			✓
IPsec VPN to FortiSASE using IKEv2, Preshared Key, and Local user	✓	✓			✓
Network lockdown	✓	✓			
Pre-logon VPN	✓				
Show zero trust network access (ZTNA) tags on FortiClient	✓	✓	✓	✓	✓
Split DNS	✓	✓			✓ For split-tunnel VPN, DNS request can be routed to the split-tunnel VPN via DNS suffix.
FSSO					
FortiClient SSO mobility agent	✓	✓			

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
Protection					
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		✓	✓		
Vulnerability scan	✓	✓	✓		
Vulnerability scan - event-based scan	✓	✓	✓		
Sandbox					
Sandboxing - on-premise and FortiSASE Cloud Sandbox	✓	✓		✓ On-premise only	
ZTNA					
ZTNA remote access	✓	✓	✓		
ZTNA tagging rules	✓	✓	✓	✓	✓

* Requires Advanced or Comprehensive subscription

SSL VPN remote user connectivity

The following table lists the FortiClient platform and version and each version's corresponding features that FortiSASE supports for SSL VPN remote user connectivity:

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
Diagnostic logs on-demand requests from FortiSASE	✓				
Digital experience monitoring agent*	✓	✓			
FortiGuard Forensics Analysis*	✓				
Access					
Autoconnect to FortiSASE using Microsoft Entra ID credentials	✓				
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓	✓		✓	✓
Bypass FortiSASE using application-based split tunnel	✓				
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via DNS server	✓	✓	✓		
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via DHCP server	✓	✓	✓		
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via local subnet	✓	✓	✓		

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net via ping server	✓	✓	✓		
Exempt endpoint from FortiSASE autoconnect when endpoint is on-net 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	✓	✓	✓	✓	✓

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
					FortiClient (iOS) does not disable the *VPN* button instantly. You must navigate away from the *VPN* page to disable the *VPN* button.
Network lockdown	✓	✓			
Pre-logon VPN	✓				
Show zero trust network access (ZTNA) tags on FortiClient	✓	✓	✓	✓	✓
Split DNS	✓	✓			✓ For split-tunnel VPN, DNS request can be routed to the split-tunnel VPN via DNS suffix.
SSL VPN connection remains active after endpoint has been idle	✓	✓	✓		
SSL VPN support for DTLS**	✓	✓		✓	✓
SSL VPN to FortiSASE			✓	✓	✓
FSSO					

Feature	Windows 7.2.13	macOS 7.2.13	Linux 7.0.13	Android	iOS
FortiClient SSO mobility agent	✓	✓			
Protection					
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		✓	✓		
Vulnerability scan	✓	✓	✓		
Vulnerability scan - event-based scan	✓	✓	✓		
Sandbox					
Sandboxing - on-premise and FortiSASE Cloud Sandbox	✓	✓		✓ On-premise only	
ZTNA					
ZTNA remote access	✓	✓	✓		
ZTNA tagging rules	✓	✓	✓	✓	✓

[*] Requires Advanced or Comprehensive subscription

[**] 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
SIA for FortiClient agent-based remote users on page 29	Secure access to the internet using FortiClient agent.
SIA for FortiExtender site-based remote users on page 29	Secure access to the internet using Thin Edge FortiExtender device as FortiSASE LAN extension.
SIA for FortiGate SD-WAN secure edge site-based remote users on page 30	Secure access to the internet using FortiGate SD-WAN Secure Edge device as FortiGate SD-WAN Secure Edge device as FortiSASE LAN extension.
SIA for FortiAP site-based remote users on page 30	Secure access to the internet using FortiAP device as FortiSASE edge device.
SIA for Branch On-ramp site-based remote users on page 30	Secure access to the internet using an IPsec device acting as an on-ramp to FortiSASE.
Log forwarding on page 31	Forward logs to an external server, such as FortiAnalyzer.
Central management using FortiManager on page 31	Centrally manage FortiSASE configuration settings from FortiManager
ZTNA on page 31	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases.
SPA using a FortiGate SD-WAN hub on page 32	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network.
SPA using a FortiSASE SPA hub on page 33	Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW).
SPA using FortiGate SASE bundle subscription on page 33	Seamless integration of FortiGate with FortiSASE for SPA to simplify the journey from SD-WAN to SASE.
SPA using a FortiSASE SPA hub with Fabric overlay orchestrator on page 34	Access to private company-hosted applications behind the FortiGate NGFW using Fabric Overlay Orchestrator.
SPA for an MSSP hub on page 35	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.
Data protection using FortiCASB on page 35	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 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 36 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 per FortiGate. All FortiGate F- and G-series desktop platforms including FortiWiFi from the 40 series to the 100 series that support virtual domains (VDOM) running FortiOS 7.4.2 and later can support FortiSASE Secure Edge connectivity. See the FortiGate model-specific datasheet to confirm VDOM support.

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 per FortiAP. This feature supports FortiAP devices running FortiAP firmware 7.2.4 and later:

- FortiAP 23JF, 234F, 432FR, 831F
- FortiAP 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 Branch On-ramp site-based remote users

FortiSASE Branch 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 subscriptions applied:

- Advanced or Comprehensive subscription
- FortiSASE Branch On-ramp Location subscription corresponding to the Advanced or Comprehensive license

See the FortiSASE Ordering Guide.

Branch On-ramp and SPA share BGP configuration. You must configure the SPA network configuration before deploying a Branch On-ramp location but you can create SPA service connections after deploying a Branch On-ramp location.

The FortiSASE Branch On-ramp Location subscription has these features:

- IPsec connectivity to a number of FortiSASE On-Ramp security PoPs (2 to 20) depending on the number of seats that the subscription specifies.
- 1 Gbps of shared bandwidth for up to 2000 simultaneous dialup IPsec connections from the IPsec device to the selected FortiSASE locations.
- 50 TB of data transfer per year based on 50 Mbps usage during business hours. Data transfer is aggregated at the account level and shared with remote users (250 GB per user). Additional data transfer subscriptions can be purchased if required. See the FortiSASE Service Description on the Fortinet Support portal.
- The Branch On-ramp Connection add-on subscription is discontinued after 25.3.b.
- FQDN and static IP address to use for each IPsec On-Ramp location

You must purchase the subscription multiple times if the expected bandwidth exceeds 1 Gbps for the location.

Existing customers can contact their Fortinet Sales or Partner representative for assistance with co-terming an existing Branch On-ramp Location subscription to support additional On-Ramp locations.

Supported Branch On-ramp IPsec devices

Device	Supported firmware version
FortiGate	7.2.8 or later

For FortiSASE Mature, the FortiGate is the only supported IPsec device that you can use for Branch 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.

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.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

SPA Service Connection subscription

A single SPA Service Connection subscription 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 35.

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 subscription 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 subscription per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection subscription and SPA FortiCloud account prerequisites on page 32.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

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

Product	Supported firmware version
FortiGate	• 7.0.10 or later • 7.2.4 or later • 7.4.0 or later

Product	Supported firmware version
	• 7.6.0 or later
FortiManager	• 7.2.0 or later, which supports SD-WAN overlay templates • 7.0.3 or later, which includes BGP and IPsec VPN recommended templates for SD-WAN overlays • 7.4.0 or later
FortiClient	7.2.13

SPA using a FortiSASE SPA hub

This use case requires a subscription per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection subscription and SPA FortiCloud account prerequisites on page 32.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

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

Product	Supported firmware version
FortiGate	• 7.0.10 or later • 7.2.4 or later • 7.4.0 or later • 7.6.0 or later
FortiClient	7.2.13

SPA using FortiGate SASE bundle subscription

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

The FortiGate SASE Bundle subscription 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 subscription.

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 subscriptions. The number of included remote user seats and available FortiSASE security points of presence (PoP) depends on the model of G-series FortiGate licensed, outlined as follows:

Model	Included remote user seats for each model	Number of security PoPs available
Below 120G	None	N/A
120G to 600G	10	2
900G to 1500G	50	2 to 4
1800G+	100	
VM and Cloud	None	N/A

The number of remote user seats are cumulative and based on the number and model of FortiGates that have the FortiGate SASE bundle subscription applied under the same FortiCloud account as FortiSASE. For example, consider that a customer purchases the FortiGate SASE bundle subscription 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). In addition, as the total number of remote user seats is 50 and above, the number of available FortiSASE security PoPs to choose from is between 2 to 4.

See the FortiSASE Ordering Guide.

SPA using a FortiSASE SPA hub with Fabric overlay orchestrator

This use case requires a subscription per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection subscription and SPA FortiCloud account prerequisites on page 32.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

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

Product	Supported firmware version
FortiGate	• 7.2.4 or later • 7.4.0 or later • 7.6.0 or later
FortiClient	7.2.13

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

Product	Supported firmware version
FortiGate	• 7.4.5 and later • 7.6.0 and later

SPA for an MSSP hub

For MSSPs using FortiCloud Organizations to arrange accounts into a root organizational unit (OU) and sub-OUs and where many tenants share a FortiGate SPA hub, FortiSASE supports tenants within a sub-OU inheriting SPA subscriptions 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 subscriptions registered in the tenant sub-OU account and the number of SPA subscriptions registered in the root OU, up to a maximum of 12 SPA subscriptions 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 subscription. The add-on subscription must be registered in the same FortiCloud account as FortiSASE. FortiSASE supports FortiCASB 24.4.b.

Language support

The following languages are supported for the FortiSASE Mature portal:

- English

Resolved issues

The following issues have been fixed in version 25.3.175 Mature unless noted otherwise. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
1224336	Added option *Disable native Windows captive portal* prompt, which when set as disabled by default, ensures that when Network Lockdown is enabled, WiFi does not disconnect after the agent tunnel disconnects. This issue was resolved in 25.4.b Mature.

Known issues

Known issues are organized into the following categories:

- New known issues on page 37
- Existing known issues on page 37

For inquiries about a particular bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 25.3.175 Mature.

Existing known issues

The following issues were identified in a previous version and remain in 25.3.175 Mature. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
716833	FortiClient (macOS) does not support application-based split tunnel.
881859	Application Control block replacement page does not work.
1120255	When changing subnet in *IP pools for tunnel and edge devices* to a more summarized subnet or supernet, observed this supernet cannot be advertised from SPA hub, which prevents access to its private networks. **Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance.
1121555	You cannot configure local IP address 10.255.1.1 as BGP peer IP address on a private access connection. **Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance.
1122059	Unable to create a policy when SSL Inspection is not set for Deep Inspection while Video Filter is Enabled. **Workaround**: Video Filter requires Deep Inspection and cannot be enabled otherwise. Therefore, set *SSL Inspection* to *Deep Inspection*, disable *Video Filter*, and set *SSL Inspection* to either *Certificate Inspection* or *No Inspection*.
1122060	Unable to disable Video Filter when SSL Inspection is not set for *Deep Inspection*.

Bug ID	Description
	Workaround: Video Filter requires Deep Inspection and cannot be enabled otherwise. Therefore, set *SSL Inspection* to *Deep Inspection*, disable *Video Filter*, and set *SSL Inspection* to either *Certificate Inspection* or *No Inspection*.
1122595	Agentless zero trust network access private application or bookmark access fails to work as expected intermittently for instances where the number of entitled security PoPs exceeds 16 and/or if any entitled PoPs have been provisioned to exceed the default maximum number of remote agents per region of 4096 (/20)
1138818	You cannot use special characters in SAML group names.
1152032	When there are more than 30000 endpoints, user cannot export all endpoints due to *Failed to download CSV* error.
1155528	Local users are not matched in created policies and are only matched if they are in a local group. **Workaround**: create a local group with just the local user and specify that group in policies.
1159200	You cannot see entire group list when searching user groups from SAML provider.
1160468	FortiClient Android - IPsec VPN IKE2 using PSK and SAML SSO (EAP enabled) is not supported
1163016	*Certificate probe failure* option in SSL inspection profile does not apply to *Certificate Inspection*.
1167710	FortiSASE does not save ZTNA tagging rule for not having macOS FileVault disk encryption.
1174053	Incorrect Identity & Access Management account ID displays on the GUI when the same user logs in with multiple tenant instances.
1174911	*FortiView Policies* widget shows incorrect destination IP address count and policy ID matching.
1176542	*Network > Managed Endpoints* refresh button does not refresh tunnel status.
1178511	*Malware Scheduled Scan* should be scheduled to run weekly instead of monthly.
1181503	Microsoft Teams and Outlook applications lose connectivity upon connecting to SWG SSO. **Workaround**: Open a new FortiCare Support ticket to obtain a custom PAC file to exclude the FQDNs required by Microsoft.
1186202	In *Managed Endpoints*, cannot filter multiple Source IP addresses with the *negate* option.
1188316	*DEM Trial* profile created not visible in *Configuration > Profiles*.
1239591	After a Mature to Feature migration, on a migrated FortiSASE instance with enhancements to analytics and logging services, all scheduled reports may get disabled and email groups may get removed unexpectedly.

Bug ID	Description
	Workaround: After the migration, reconfigure scheduled reports and email groups, if needed.
1207211	DLP does not block a file when uploaded to Outlook or WeTransfer.

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 subscription 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 subscription 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.
- When installing FortiClient on Windows, user may see a warning about FortiClient originating from an unknown publisher if Windows Defender is enabled.
- Digital experience monitoring (DEM) on previously connected Windows endpoint does not work after reprovisioning FortiSASE instance. To restore DEM functionality, reinstall FortiClient and the DEM agent together on the Windows endpoint.
- For FortiClient (macOS) endpoint management connections to be successfully established with FortiSASE Endpoint Management Service, in FortiSASE you must create a policy with deep inspection disabled for Fortinet infrastructure destinations (Fortinet-FortiSASE, Fortinet-FortiCloud, Fortinet-FortiClient.EMS, and Fortinet-FortiSandbox.Cloud) to exempt this traffic.

⚠ 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.

When enabling Sandbox in an endpoint profile, and when using a FortiSASE-managed endpoint running FortiClient (macOS) and Microsoft Defender, you must enable passive mode on Microsoft Defender.

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.
- SSO authentication is strongly recommended for SWG users.
- 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