# Release Notes

## FortiSASE 25.3.148 Feature

**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

November 07, 2025
FortiSASE 25.3.148 Feature Release Notes
72-253139F-1170483-20251107

# TABLE OF CONTENTS

# Change log

| Date | Change description |
|---|---|
| 2025-10-09 | Initial release. |
| 2025-10-14 | Updated New known issues on page 41. |
| 2025-10-22 | Initial release of 25.3.148. |
| 2025-10-28 | Updated Product integration and support on page 21 and What's new for 25.2.24 (25.2.a) on page 13. |
| 2025-10-29 | Updated New known issues on page 41. |
| 2025-10-30 | Updated Product integration and support on page 21. |
| 2025-11-05 | Updated Special notices on page 17. |
| 2025-11-07 | Updated What's new on page 7. |

# Introduction

This document provides a list of new features and changes and known issues for FortiSASE 25.3.148 Feature. Review all sections of this document before using this service.

# What's new



# What's new preview for 25.4.a Feature

This is a What's new preview for the next FortiSASE release. Please note that any support tickets raised for additional questions will not be considered.

Other than this preview section, FortiSASE documentation still reflects the current 25.3.148 (25.3.c.1) release and will be updated at the end of the FortiSASE maintenance window.

For details about FortiSASE maintenance, see Appendix E - Monthly Maintenance.

- Added support for Public Cloud security PoPs: Buenos Aires - Argentina, Lima - Peru, London - United Kingdom, St. Ghislain - Belgium, Warsaw - Poland, Zurich - Switzerland.

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

25.3.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

# What's new for 25.3.139 Feature (25.3.c Feature)

- Support FortiClient 7.2.12 as the recommended version for FortiSASE desktop users. See Product integration and support on page 21.
- Added support for using a custom domain and a certificate for the custom domain that can be used to access a ZTNA private application. The administrator must configure the custom domain DNS CNAME record with the FortiSASE private application domain for the private application. See Configuring a private application.
- Added a built-in custom PAC file editor for creating and editing PAC files hosted on FortiSASE.
  - These hosted PAC files can be downloaded or referenced via its hosted URL by Proxy (formerly SWG) users.
  - Each FortiSASE instance supports a maximum of 32 hosted PAC files.

  See Customizing the PAC file.
- For FortiSASE instances with Proxy (formerly SWG) enabled, added a best practice recommendation to migrate to Secure Proxy using HTTPS connections. Hosted PAC files will be updated as part of the migration.
  - After the migration, to ensure Proxy user functionality, custom PAC files maintained by administrators themselves must be edited to support Secure Proxy and redeployed on Proxy endpoints.

  See Secure proxy migration.
- Added support for additional Web Filter configuration settings including the ability to prioritize URL filter entries, logging search keywords, and displaying the FortiGuard web filter category and subcategory in a tooltip when hovering over a domain. Also, added support for synchronizing these settings using FortiManager with the central management select availability feature. See Configuring and applying a Web Filter profile.
- Added support for configuring application control filter overrides based on multiple filters including application category, behavior, popularity, protocol, risk, technology, and vendor. Also, added support for configuring actions for custom application signatures. Moreover, added support for synchronizing these settings using FortiManager with the central management select availability feature. See Application Control With Inline-CASB.
- For new instances, support has been added for a new endpoint vulnerability report based on logs collected from FortiClient endpoints. See Report types.
- For new instances, support has been added for a new Secure Private Access (SPA) report displaying the health of each connected SPA hub, the traffic through popular hubs, and the status of SD-WAN performance SLAs. See Report types.
- For new instances, support has been added for a new *Cloud Security Usage Report* to identify the total number of users in the reporting period and per PoP, the number of sessions, and total traffic. Average hourly underlay activity is reported by security PoP. Top authentication failures are listed by region and originating IP address. See Report types.
- The recommendation to use SOCaaS log forwarding is presented in the *Operations > Logs > Settings* page and through additional portal notifications. Enabling SOCaaS log forwarding is included as a best practice recommendation. See Forwarding logs to SOCaaS and Software audit & version.
- Administrator logins, configuration audit logs, and user audit logs have been introduced in the *System > Administration* page. Once the feature has been enabled, any configuration changes made by an administrator will require a change summary to be submitted. See Administration.

- The UI version has been removed from the FortiSASE portal URL, ensuring a consistent path for ease of access.
- Added support for Chicago, Illinois, USA as a Public Cloud security PoPs. See Global data centers.
- For new instances, added an Automation page in *Operation > Administration* to allow configuring of actions, such as sending alert emails, based on predefined triggers to proactively notify administrators of events. Currently, alert emails can be triggered for an unstable Secure Private Access (SPA) connection only when SLA failures, routing changes, and BGP neighbor status changes all occur. See Automation.

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

25.3.b.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

# What's new for 25.3.89 Feature (25.3.b Feature)

- 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. See New major features available.
- Added support for branch on-ramp with the Standard subscription for new and upgraded instances. 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.
- Added support for FIDO2 authentication for FortiClient agent tunnels, which is configurable in *Endpoint profiles* for the *FortiSASE Cloud Security tunnel* and custom tunnels when *Authenticate with SSO* and *Use FortiClient built-in browser for SAML authentication* are enabled. See Advanced settings.
- Added support in the *AntiVirus* security profile for content disarm and reconstruction (CDR), which sanitizes Microsoft Office documents and PDF files by removing potentially malicious and untrusted content from them (disarm) without affecting the integrity of its textual content (reconstruction). CDR does not support SMTP, FTP, and CIFS protocols. See AntiVirus.
- Added support for configuring and viewing predefined DLP sensors and DLP dictionaries managed by the *FortiGuard DLP service* in the *DLP* security profile and in *Security > Traffic > Security profiles > Profile*

*resources*, respectively. See Profile resources.

- Added support for displaying IPAM usage information in a chart in *Network > IP management > IPAM* indicating which subnets are allocated, the percentage of the IPAM pool that remains unallocated, and the percentage of each IP block allocated via DHCP. See IP management.
- Added support for displaying security PoPs, logging PoPs, and endpoint management PoPs on a map during provisioning and after provisioning in *Operations > Connectivity > Infrastructure*. See Infrastructure.
- Added support for synchronizing firewall policies, firewall proxy policies, firewall schedules and security posture tags from FortiManager to FortiSASE using the central management select availability feature. See Configuring settings using policy packages in FortiManager.
- Added support for Auckland, New Zealand as a Public Cloud security PoP. See Global data centers.
- Added support for Perth, Australia as a Public Cloud security PoP. See Global data centers.
- Added support for Delhi, India as a Public Cloud security PoP. See Global data centers.

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

25.3.a.3 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

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

25.3.a.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

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

25.3.a.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

# What's new for 25.3.40 Feature (25.3.a Feature)

- Enhancements for Digital Experience Monitoring (DEM), including a path diagram for endpoint traceroute results, support for displaying additional SaaS monitoring metrics, and customizing the list of SaaS applications to monitor. See Digital Experience Monitoring.
- Updated log retention period for newly provisioned instances to FortiView, Log View, and Report functions to seven days. See Log retention policy.
- Added support for secure explicit proxy. Secure explicit proxy is enabled by default when enabling proxy for newly provisioned instances. Instances provisioned before 25.3.a have the option to enable secure explicit proxy. See Proxy configuration.

- Added support for configuring an action to inspect or block QUIC traffic for agent and Edge device traffic. See Configuring an action for QUIC traffic.
- Added support for configuring additional trusted remote gateways as failover options alongside the FortiSASE Cloud Security tunnel, with the ability to define their connection priority order within each endpoint profile. See Advanced settings.
- Added support for Secure Private Access (SPA) application monitoring, allowing up to 20 custom applications hosted behind SPA Hubs to be defined and monitored using ICMP health check probes initiated by Security PoPs to verify application availability. See SPA application monitoring.
- Added support for enabling the BGP MED options always-compare-med and deterministic-med on FortiSASE to enable selecting a preferred SPA Hub based on MED values, particularly when receiving prefixes from SPA Hubs belonging to different ASes. See BGP MED Setting.
- Added support to enable and manage communication between remote endpoints connected via the FortiSASE Cloud Security tunnel through a Secure Private Access (SPA) Hub. Administrators can enforce granular control by defining endpoint-to-endpoint policies that selectively allow specific traffic between designated endpoints. See Enabling endpoint to endpoint communication.
- Added support for administrators to schedule FortiSASE upgrades by selecting from a list of predefined maintenance window slots, directly through the FortiSASE portal. See Software audit & version.
- Added support to control and specify the public IP address used by a Security PoP to perform source NAT on remote user traffic as it exits the PoP, based on matching criteria such as user group and the originating country or region of the remote user's traffic. See IP management.
- Added support to change the isolation data limit from a user-based and monthly-based model to a tenant-based and yearly-based model. Each tenant is now entitled to a maximum amount of isolation data per year. Once this limit is exceeded, any traffic configured for isolation will be blocked for all users within the tenant. See RBI.
- Added support for configuring new security posture tagging rules, including tagging based on CVEs, using negation to identify non-vulnerable devices, and combining multiple tagging rules using logical AND/OR operators. See Security posture tags and tagging rules.
- Added support for enforcing pre-connection posture checks using security posture tags to allow or deny endpoints from establishing a connection to the FortiSASE Cloud Security tunnel based on their associated tags. See Pre-connection posture checks.
- Added support for optionally displaying a sequence number column in the policy list to help administrators manage and identify policy order using their sequence number. See Policies.
- 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.
- Added support for customizing captive portal replacement message for Edge devices. See HTML templates.
- Support FortiClient 7.2.11 as the recommended version for FortiSASE desktop users. See Product integration and support on page 21.
- Added support for Dublin, Ireland (DUB-A2) as a Public Cloud security PoP. See Global data centers.

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

25.2.c.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

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

25.2.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 39.

# What's new for 25.2.81 Feature (25.2.c Feature)

- Support FortiClient 7.2.10 as the recommended version for FortiSASE desktop users. See Product integration and support on page 21.
- Added a new audit page providing configuration best practice recommendations. See Software audit & version.
- For new FortiSASE tenants created after 25.2.c, support dedicated public IP addresses for FortiSASE tenants with the Standard subscription without additional licensing.
- RBI now supports isolation for the following categories only. See RBI.
  - Unrated
  - Newly Observed Domain
  - Newly Registered Domain
  - Malicious Websites
- FortiSASE has added powerful new capabilities that are enabled by default on new instances created after the 25.2.c release. For 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 (including mobile), 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 39.

# 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 39.

# What's new for 25.2.45 (25.2.b)

- FortiSASE now supports Branch On-ramp deployment for up to 20 On-Ramp security PoPs.
- 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 39.

# 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 remote agent connectivity. See Product integration and support on page 21.
- 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 security PoPs. See Appendix A - FortiSASE data centers.
- Added support for registering FortiCASB data protection add-on subscriptions. See Product integration and support on page 21.
- 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 support for Querétaro, Mexico and Sydney, Australia as Public Cloud security PoPs. See Global data centers.
- Added support for Sao Paulo, Brazil as a Fortinet Cloud security PoP. 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 security PoPs 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 On-ramp tunnel.
- 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 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 32.
- Added datacenter support for Madrid, Spain as a Fortinet Cloud security PoP. 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 39.

# 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 39.

# 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 agent and proxy 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 agent and proxy policies using FortiManager with the central management select availability feature. See Central Management.
- Added support for adding administrator-defined comments to agent and proxy 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 support for Plano, Texas, USA as a Fortinet Cloud security PoP. 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 PoPs 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:
    - Proxy
    - 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 security PoPs
  - Other custom changes to the instance have not been made.

# Special notices

## On-shore Dubai customers

The DXB-F2 Fortinet Cloud security PoP 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 security PoP. See Global data centers.

## Removable media access

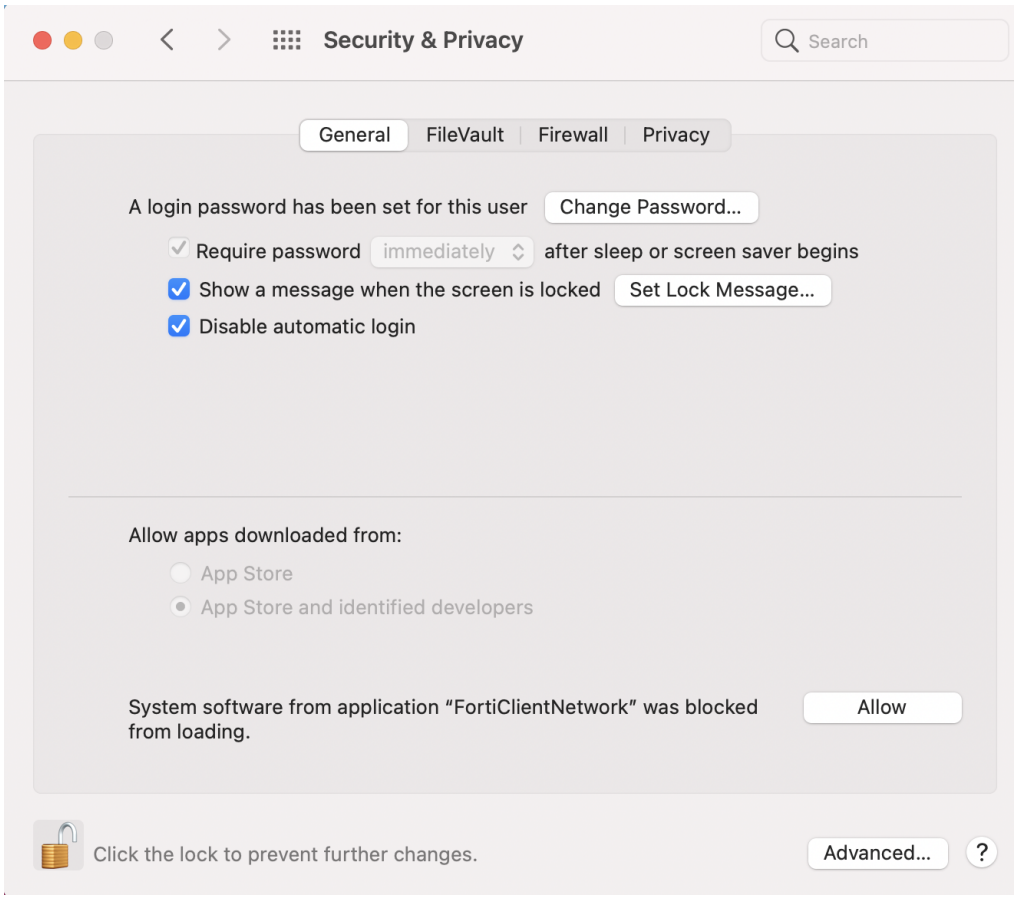
The *Profile > Removable Media Access Control* option only works if you enable Malware Protection, an optional feature, when installing FortiClient on the endpoint.

## Activating the FortiClientNetwork extension

After you connect FortiClient (macOS) to FortiSASE, attempts to connect to SSL tunnels 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.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) 7.2.12
- FortiClient (macOS) 7.2.12
- FortiClient (Linux) 7.0.13
- FortiClient (Android)
- FortiClient (iOS)

FortiClient 7.2.12 is the recommended version for FortiSASE for desktop users. FortiSASE has updated installers and download links to use FortiClient 7.2.12.

- 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. FortiSASE only supports patch versions within FortiClient 7.2.

# Considerations

- For existing instances created before 24.4.b.1 with remote user connectivity to FortiSASE using SSL, the recommended version is FortiClient 7.2.12.
- Starting in FortiSASE 24.4.b.1, IPsec remote agent support is enabled by default on new instances.
  - For instances with IPsec remote user support enabled, the recommended version is FortiClient 7.2.12.
  - For instances created before 24.4.b.1, implementing IPsec 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 remote user support implementation without significant data loss and service disruption.
  - Fortinet recommends that you only raise a request to implement IPsec remote user support after careful consideration and understanding of impact and service disruptions.

# 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 7.2.12 | macOS 7.2.12 | 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 7.2.12 | macOS 7.2.12 | 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 | ✓ | ✓ | ✓ | | |
| Configurable MTU on IPsec tunnel | ✓ | ✓ | | | |
| Endpoint profile assignment based on Microsoft Entra ID groups | ✓ | | | | |
| Endpoint profile change notifications | ✓ | ✓ | ✓ | | |
| Endpoint telemetry | ✓ | ✓ | ✓ | ✓ | ✓ |
| Endpoint tunnel connectivity notifications | ✓ | ✓ | ✓ | | |
| Endpoint tunnel disconnection by disabling management connection from FortiSASE | ✓ | ✓ | ✓ | | |
| External browser as user-agent for SAML login | ✓ | ✓ | ✓ | ✓ | ✓ |
| Force always on tunnel | ✓ | ✓ | ✓ | ✓ | ✓ |

| Feature | Windows 7.2.12 | macOS 7.2.12 | 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 tunnel | ✓ | | | | |
| Show security posture tags on FortiClient | ✓ | ✓ | ✓ | ✓ | ✓ |
| Split DNS or DNS redirection** | ✓ | ✓ | | | ✓<br>For split-tunnel VPN, DNS request can be routed to the split-tunnel VPN via DNS suffix. |
| **FSSO** | | | | | |
| FortiClient SSO mobility agent | ✓ | ✓ | | | |
| **Protection** | | | | | |

| Feature | Windows 7.2.12 | macOS 7.2.12 | Linux 7.0.13 | Android | iOS |
|---|---|---|---|---|---|
| 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** | | | | | |
| Security posture tagging rules | ✓ | ✓ | ✓ | ✓ | ✓ |
| ZTNA remote access | ✓ | ✓ | ✓ | ✓ HTTPS proxy access support via EMS and MDM integration | ✓ HTTPS proxy access support via EMS and MDM integration |

* Requires Advanced or Comprehensive subscription

** You can achieve split DNS or DNS redirection for Linux, iOS, and Android with transparent DNS redirection, which is available with the Feature release.

# 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 7.2.12 | macOS 7.2.12 | 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 7.2.12 | macOS 7.2.12 | 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 | ✓ | ✓ | ✓ | | |
| Configurable MTU on IPsec tunnel | ✓ | ✓ | | | |
| Endpoint profile assignment based on Microsoft Entra ID groups | ✓ | | | | |
| Endpoint profile change notifications | ✓ | ✓ | ✓ | | |
| Endpoint telemetry | ✓ | ✓ | ✓ | ✓ | ✓ |
| Endpoint tunnel connectivity notifications | ✓ | ✓ | ✓ | | |
| Endpoint tunnel disconnection by disabling management connection from FortiSASE | ✓ | ✓ | ✓ | | |
| External browser as user-agent for SAML login | ✓ | ✓ | ✓ | ✓ | ✓ |
| Force always on tunnel | ✓ | ✓ | ✓ | ✓ | ✓ |

| Feature | Windows 7.2.12 | macOS 7.2.12 | 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 tunnel | ✓ | | | | |
| Show security posture tags on FortiClient | ✓ | ✓ | ✓ | ✓ | ✓ |
| Split DNS or DNS redirection** | ✓ | ✓ | | | ✓ For split-tunnel VPN, DNS request can be routed to the split-tunnel VPN via DNS suffix. |
| SSL tunnel connection remains active after endpoint has been idle | ✓ | ✓ | ✓ | | |
| SSL tunnel support for DTLS*** | ✓ | ✓ | | ✓ | ✓ |
| SSL tunnel to FortiSASE | ✓ | ✓ | ✓ | ✓ | ✓ |
| **FSSO** | | | | | |
| FortiClient SSO mobility agent | ✓ | ✓ | | | |

| Feature | Windows 7.2.12 | macOS 7.2.12 | Linux 7.0.13 | Android | iOS |
|---|---|---|---|---|---|
| **Protection** | | | | | |
| Antiransomware | ✓ | | | | |
| Next generation antivirus (AV) – real-time AV and cloud malware protection | ✓ | ✓ | ✓ | | |
| Removable media access control | ✓ | ✓<br>FortiClient (macOS) does not support rules. It only supports allow and block actions. | ✓<br>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 | ✓ | ✓ | | ✓<br>On-premise only | |
| **ZTNA** | | | | | |
| Security posture tagging rules | ✓ | ✓ | ✓ | ✓ | ✓ |
| ZTNA remote access | ✓ | ✓ | ✓ | ✓<br>HTTPS proxy access support via EMS and MDM integration | ✓<br>HTTPS proxy access support via EMS and MDM integration |

* Requires Advanced or Comprehensive subscription

** You can achieve split DNS or DNS redirection for Linux, iOS, and Android with transparent DNS redirection, which is available with the Feature release.

# 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 31 | Secure access to the internet using FortiClient agent. |
| SIA for FortiExtender site-based remote users on page 31 | 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 32 | 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 32 | Secure access to the internet using FortiAP device as FortiSASE edge device. |
| SIA for Branch On-ramp site-based remote users on page 33 | Secure access to the internet using an IPsec device acting as an on-ramp to FortiSASE. |
| Log forwarding on page 33 | Forward logs to an external server, such as FortiAnalyzer. |
| Central management using FortiManager on page 34 | Centrally manage FortiSASE configuration settings from FortiManager |
| RBI on page 34 | For proxy users, isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container. |
| ZTNA on page 34 | 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 35 | Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network. |
| SPA using a FortiSASE SPA hub on page 36 | Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW). |
| SPA using FortiGate SASE bundle subscription on page 36 | Seamless integration of FortiGate with FortiSASE for SPA to simplify the journey from SD-WAN to SASE. |

| Use case | Description |
|---|---|
| SPA using a FortiSASE SPA hub with Fabric overlay orchestrator on page 37 | Access to private company-hosted applications behind the FortiGate NGFW using Fabric Overlay Orchestrator. |
| SPA for an MSSP hub on page 37 | Access to private company-hosted applications behind the FortiGate secure private access (SPA) hub shared in a managed security service provider (MSSP), multitenant environment. |
| Data protection using FortiCASB on page 38 | 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 | | | ✓ | ✓ |

| Feature | FortiExtender 200F | FortiBranchSASE 20G | FortiBranchSASE 20G WiFi | FortiBranchSASE 10F WiFi |
|---|---|---|---|---|
| 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 39 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 below 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
- FortiAP 23JK, 231K, 241K, 243K, 441K, 443K

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 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:

- Standard, Advanced, or Comprehensive subscription
- FortiSASE Branch On-ramp security PoP subscription corresponding to the Advanced or Comprehensive license

See the FortiSASE Ordering Guide.

When using FortiGate branch devices, BGP configuration is shared between the Branch On-ramp and SPA features.

- You must configure the SPA network configuration first before deploying a Branch On-ramp security PoP but you can create SPA service connections after deploying a Branch On-ramp security PoP.
- For this use case, only iBGP is supported between the FortiGate branch devices and Branch On-ramp Security PoP.

Since BGP is not supported when using third-party branch devices, you must configure static routing on the branch device.

The FortiSASE Branch On-ramp Location subscription 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 security PoPs
- 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 security PoP
- Enable connectivity from different IPsec device types, such as FortiGate or third-party IPsec devices

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

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 security PoPs.

# 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. FortiSASE supports using FortiManager 7.6 or FortiManager Cloud 7.6 for central management when using FortiManager 7.6.4 or later.

- The central management feature requires FortiManager 7.4.4 or later for synchronizing configuration settings other than policy packages.
- The policy packages feature requires either FortiManager 7.4.8 or later, or FortiManager 7.6.4 or later for synchronizing policy packages.
- 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 or Comprehensive remote users subscription to use remote browser isolation (RBI) with the following limitations:

- Supported for proxy 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 overlays and BGP.

# 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 37.

# 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 license and SPA FortiCloud account prerequisites on page 35.

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

| Product | Supported firmware version |
|---|---|
| FortiGate | • 7.0.10 or later<br>• 7.2.4 or later<br>• 7.4.0 or later<br>• 7.6.0 or later |
| FortiManager | • 7.2.0 or later, which supports SD-WAN overlay templates<br>• 7.0.3 or later, which includes BGP and IPsec recommended templates for SD-WAN overlays<br>• 7.4.0 or later |
| FortiClient | 7.2.12 |

# 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 license and SPA FortiCloud account prerequisites on page 35.

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

| Product | Supported firmware version |
|---|---|
| FortiGate | • 7.0.10 or later<br>• 7.2.4 or later<br>• 7.4.0 or later<br>• 7.6.0 or later |
| FortiClient | 7.2.12 |

# 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 license and SPA FortiCloud account prerequisites on page 35.

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<br>• 7.4.0 or later<br>• 7.6.0 or later |
| FortiClient | 7.2.12 |

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<br>• 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.

# Resolved issues

The following issues have been fixed in version 25.3.148 Feature. For inquiries about a particular bug, contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 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. |
| 1128030 | In some cases, when connecting a thin-edge FortiGate for the first time, the device does not initialize properly, causing subsequent configuration failure. |
| 1138818 | You cannot use special characters in SAML group names. |
| 1147700 | Unable to set action for FQDN Feeds and custom entry in custom webfilter profile. |
| 1153197 | SSL tunnel traffic to secure private access (SPA) resource (FQDN domain) via split DNS rule may fail to match firewall policy that uses FQDN-based address. |
| 1163016 | SSL inspection profile `cert-probe-failure` does not apply on certificate inspection. |
| 1167710 | FortiSASE does not save security posture tagging rule for not having macOS FileVault disk encryption. |
| 1168623 | *Bandwidth Monitor* incorrectly shows transmit and receive values as 0 bps. |
| 1174053 | Incorrect Identity & Access Management account ID displays on the GUI when the same user logs in with multiple tenant instances. |
| 1174881 | When onboarding a new user with local user option, the password reset feature via the user portal does not work. This can result in tunnel connection failure if the user resets the password via the user portal. |
| 1176542 | *Operations > Endpoints* refresh button does not refresh tunnel status. |
| 1177895 | The GUI does not combine licenses with the same user seat count in *System > License Overview*. |
| 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. |
| 1185223 | The GUI still shows previously expired license even though the license is already renewed in *System > License Overview*. |
| 1191733 | Inline CASB not working for login.live.com. |
| 1196243 | *Default* endpoint profile missing default exclusions in *Steering bypass destinations*. |
| 1198312 | Synchronizing Entra ID domain from *Domains* page never completes and remains stuck at 40%. |

| Bug ID | Description |
|---|---|
| 1198682 | IAM users are unable to access the FortiSASE portal, prompting the error *An error occurred during FortiSASE startup. You will be logged out*. |
| 1200291 | A site creation after a site deletion can lead to configuration loss due to missing meta data. |
| 1205125 | Unable to create new on-ramp PoP for account with source IP anchoring. |
| 1207741 | Unable to increase number of on-ramp tunnel connections beyond 10 and observe error *An error occurred, Request connection limit exceeded. Total allow connections: 20*. |
| 1209754 | After upgrading MSSP root account to Feature version, the MSSP admin may not be able to login to tenant account that have not upgraded to Feature version yet. |
| 1211785 | MSSP root accounts without a FortiSASE license applied cannot login to the FortiSASE portal and see a *Missing entitlements* error. |
| 1213916 | VPN and Proxy SSO authentication fails to work if the administrator clicks Apply in the Endpoints Profiles > Global Connection Settings page. |

# Known issues

Known issues are organized into the following categories:



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

## New known issues

The following issues have been identified in version 25.3.148 Feature. For inquiries about a particular bug, contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 1213936 | IPsec SAML SSO authentication fails intermittently on some security PoPs within the same FortiSASE instance.<br>**Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance. |

## Existing known issues

The following issues were identified in a previous version and remain in 25.3.148 Feature. 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. |
| 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) |
| 1138018 | Cannot download preconfigured installer from FortiSASE portal due to *No link found for the specified OS* error. |
| 1146409 | Agentless RBI does not work when SWG SSO is configured. |

| Bug ID | Description |
|---|---|
| | **Workaround**: Ensure the security profile group used for the "CSP_REPORT" proxy policy is using certificate inspection instead of deep inspection. |
| 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.<br>**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. |
| 1174911 | *FortiView Policies* widget shows incorrect destination IP address count and policy ID matching. |
| 1177840 | Cannot submit FortiGuard Forensics Analysis request for endpoint when *Reason for escalation is set to Other due to Error creating forensics request. Bad request*. |
| 1179359 | API-based CASB region selection does not display *Europe* region in dropdown selection. |
| 1184436 | FortiBranchSASE endpoints do not receive network traffic after successful authorization even though the device appears online. |
| 1195155 | Cannot access API-Based CASB *Applications* and *Data Protection* pages, which keep loading and return the error *Failed to fetch patterns* in the capture tool. |
| 1196263 | Failed to upgrade edge device FortiAP 431F/231F firmware version from 7.2 to 7.4. |
| 1196551 | FortiGuard Category Based Filter still enabled in FortiSASE when corresponding setting in FortiManager was disabled and central management synchronized successfully. |
| 1200719 | Requesting FortiClient diagnostic and debug logs from endpoints returns *Failed to request logs from the endpoint*. |
| 1205320 | Client does not receive an IP address via DHCP when connected to FortiGate as FortiSASE LAN extension. |
| 1205444 | Unable to configure Agentless ZTNA on an Advanced license instance despite having a dedicated IP already assigned. |
| 1205675 | When using BGP on loopback for SPA, the FSSO connection to FortiAuthenticator is not being sourced by the loopback IP or Security PoP IPs. |
| 1210149 | Renaming the security profile group to *no-inspection* fails with an *Internal Server Error: Internal error when processing the request. Failed to save < original profile group name >*. Attempting to access the original security profile group afterward results in *Failed to get SSL inspection information*. |
| 1211502 | New custom IPsec tunnels do not work due to a missing default SAML 443 port set in the endpoint profile.<br>**Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance. |

| Bug ID | Description |
|---|---|
| 1213309 | When multiple groups are defined with the same name in Entra ID, the wrong user group ID is assigned to an Agent SSO remote group. |
| 1213916 | VPN and Proxy SSO authentication fails to work if the administrator clicks *Apply* in the *Endpoints Profiles > Global Connection Settings* page.<br>**Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance. |

# 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, tunnel 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 tunnel, the FortiSASE environment must have at least one SSL tunnel 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, tunnel 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.

Using alternate tunnel 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 proxy and proxy single sign on (SSO) to configure agentless zero trust network access (ZTNA), you do not need to configure the remote user endpoints for proxy. 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 proxy and proxy SSO for remote user authentication.

When you enable a valid agent or proxy configuration on a FortiSASE instance, an endpoint enabled with matching remote agent or proxy 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 tunnel or proxy traffic flow. This aligns with the agentless ZTNA use case where the user accesses a private application without connecting to FortiSASE as an agent or proxy user. Therefore, for valid agent or proxy 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 proxy users.
- Deauthenticating a proxy SSO user does not direct user to reauthenticate on device without clearing browser cache first.
- For proxy SSO users, to properly proxy legacy Skype traffic, bypass SSO authentication by customizing the PAC file. See Customizing the PAC file.
- For proxy SSO users, at least one proxy 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 proxy SSO users that is destined for hosts or URL categories defined as deep inspection exemptions does not work.
  - You must not configure proxy policies using SSO authentication with certificate inspection.
  - If certificate inspection is required in a proxy policy, then SSO authentication must not be configured in that policy.
- LDAP authentication is unavailable for remote agents using IPsec tunnels.
  **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.

# Policies

For SSL remote agents, whenever changes are made to an existing policy, they take effect only after SSL agents reconnect to FortiSASE.

www.fortinet.com