Release Notes

FortiSASE 26.1.107 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

May 22, 2026
FortiSASE 26.1.107 Feature Release Notes
72-261107F-1170483-20260522

TABLE OF CONTENTS

Change log

Date	Change description
2026-05-22	Initial release.

Introduction

This document provides a list of new features and changes and known issues for FortiSASE 26.1.107 Feature. Review all sections of this document before using this service.

What's new

*Infrastructure change only

What's new for 26.1.107 (26.1.2.2 Feature)

- For new instances and existing users already on FortiClient 7.4.6, support has been added for FortiClient 7.4.7 for FortiSASE desktop users. See Supported FortiClient 7.4.7 features on page 29.
- Added support for external feeds and FSSO features when using SPA hubs configured for BGP on loopback. When an existing SPA hub configured for BGP on loopback has had its SPA service connection previously configured in 26.1.2.1 or earlier, to enable support for these features go to *Operations > Secure private access*, edit the SPA service connection, leave settings unchanged, and click *OK*. See Supported features for each SPA BGP routing design.

What's new for 26.1.99 (26.1.2.1.1 Feature)

26.1.2.1.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 50.

What's new for 26.1.97 (26.1.2.1 Feature)

- Added support for integrated management of the FortiSASE Secure Browser extension used with unmanaged and contractor devices. With the deployment of the FortiSASE Secure Browser extension, administrators can gain full visibility into browser activity without deep packet inspection (DPI), can monitor and block Web-based threats, and can prevent data exfiltration. This feature is a select availability feature in FortiSASE that is not enabled by default on new instances. If you require this feature for your new or existing FortiSASE instance, create a new ticket with FortiCare Support. See Secure Browser.
- Added support for configuring dead peer detection (DPD) settings applicable to IPsec agent tunnels via the *Global configuration settings* page to configure Security PoPs and via *Advanced* settings within an endpoint profile for the FortiSASE Cloud Security tunnel and any custom IPsec tunnels, respectively. This is a select availability feature that requires a Fortinet Support ticket to enable on new and existing instances. See IPsec dead peer detection customization.
- Remote browser isolation (RBI) is now a select availability feature and is disabled by default. See RBI.
- Added support for applying Fortinet Location and Public Cloud Location Branch On-ramp licenses to a FortiSASE instance with the Comprehensive or Advanced subscription. On-ramp locations can only be provisioned based on the licenses registered, be that a Fortinet Location or Public Cloud Location. See Appendix A - FortiSASE data centers.
- In *Endpoint management > Endpoint profiles*, when configuring the *Protection* tab details of a new or existing profile, enabling *Trigger vulnerability scan on software change* will result in a vulnerability scan occurring on the endpoint when new software is installed and detected. See Protection.

What's new for 26.1.92 (26.1.2 Feature)

- Added support for bandwidth policies and profiles used for providing bandwidth control of internet access and private access traffic. See Bandwidth control.
- The FortiClient Log Level can be customized per endpoint profile in your FortiSASE instance to simplify debug log collection. In *Endpoint management > Endpoint profiles > FortiClient GUI settings*, enabling *Allow debug log generation* will set the associated endpoints' FortiClient *Log Level* to *Debug*. This feature is disabled by default. When disabled, the *Log Level* is set to *Info*. See FortiClient GUI Settings.
- Added support for synchronizing SSO SAML IdP server settings and SSO user groups with firewall policies and firewall proxy policies. This support relies on synchronizing policy packages from FortiManager to FortiSASE using the central management select availability feature. See Central management.
- Added support for synchronizing one-time schedules with firewall policies and firewall proxy policies. This support relies on synchronizing policy packages from FortiManager to FortiSASE using the central management select availability feature. See Central management.
- Added support for Public Cloud security PoPs: Amsterdam - Netherlands, Ashburn - Virginia - USA, Chicago - Illinois - USA, Melbourne - Australia, Montreal - Canada, Osaka - Japan, Santiago - Chile, Stockholm - Sweden. See Global data centers.

What's new for 26.1.73 (26.1.1.2 Feature)

- For new instances and existing users already on FortiClient 7.4.5, support has been added for FortiClient 7.4.6 for FortiSASE desktop users. See Supported FortiClient 7.4.7 features on page 29.
- For existing instances, support has been added for FortiClient 7.2.14 for FortiSASE desktop users. See Supported FortiClient 7.2.14 features on page 34.

What's new for 26.1.40 (26.1.1.1 Feature)

- For IPsec instances, added support for updating the pre-shared key for the FortiSASE Cloud Security tunnel. This enables IPsec instances to support regional compliance rules to on-premise devices and failover sequence features. See Geofencing.
- For instances supporting IPsec and FortiClient 7.4, added support for FortiSASE Cloud Security tunnel autoconnect using the session resumption timeout. See Global connection settings.
- Added support for configuring FortiClient internet check that validates internet connectivity before agent tunnel autoconnect. See Advanced settings.
- Added support for Public Cloud security PoPs: Abu Dhabi - United Arab Emirates, Jeddah - Saudi Arabia, Milan - Italy. See Global data centers.

What's new for 26.1.26 (26.1.1 Feature)

- Added support for the new FortiGate SD-WAN Service Bundle subscription to accelerate the journey from SD-WAN to SASE. The new bundle includes a FortiSASE Starter Kit with FortiSASE Standard remote user subscriptions and secure private access (SPA) connectivity to F-series FortiGate models starting with 100F and G-series FortiGate models starting with 120G. See Common use cases.
- In endpoint profiles, added the ability to disable agent-based ZTNA functionality, also known as *ZTNA destination* on FortiClient, when this functionality conflicts with other applications on managed endpoints. See ZTNA.
- In endpoint profiles, added the ability to show only selected FortiClient tabs including *Remote Access*, *ZTNA Destination*, *Malware Protection*, *Sandbox Detection*, and *Vulnerability Scan*, and added the ability to select the default tab shown in FortiClient. Features disabled within an endpoint profile will also be disabled from being shown in FortiClient. See FortiClient GUI Settings.
- Additional log forwarding servers can be configured in the *Log Forwarding to Self-Managed Service* settings. See Forwarding logs to an external server.
- Log forwarding to FortiAnalyzer Cloud can be enabled in the *Log Settings*. This feature requires the FortiAnalyzer Cloud Storage Add-On License subscription and FortiAnalyzer 7.6.3 or later. If there is no FortiAnalyzer Cloud Storage Add-On License, token generation will not be successful. See Forwarding logs to FortiAnalyzer Cloud and the FortiAnalyzer Ordering Guide for more information.
- Added enhancements for Digital experience monitoring (DEM) SaaS monitoring:

  - Visualize DEM health measurement metrics to quickly detect health events trend. Using additional filters and time brush event control, compare health metrics across multiple SaaS applications and security PoPs.
  - Review DEM health events with additional controls, including time brush control for viewing health events within a specific time period, application and security PoP filters, and so on.
  - DEM health event incident drill down enhancements have been implemented, including metric graphs, SaaS application and security PoP user access information, health event traceroutes, and so on.

  See SaaS monitoring.
- Added the ability for customers to customize the management IP address range used for FortiExtender and LAN extension control plane subnet. This can be configured to avoid addressing conflicts with your on-prem network.
  - Prior to customization, by default, the management subnet of 10.253.0.0/16 is reserved, in addition to the subnet that is visible on the page (default: 10.252.0.0/16).
  - Once a custom subnet has been configured, the previously reserved management subnet of 10.253.0.0/16 is also removed.

  See IP management.
- Added a new maintenance window 22:00–06:00 JST (13:00 - 21:00 UTC) that is more suitable for Japanese instances. For new instances with a Japanese security PoP selected, their maintenance windows will be automatically assigned to this new window. For existing instances with a Japanese security PoP selected, administrators can select this new window from *Software audit & version > Version*. See Software audit & version.
- Added source IP anchoring support for designated Public Cloud locations whose naming convention includes -O or -A. See Global data centers.
- Added support for Public Cloud security PoPs: Bogota - Colombia, Frankfurt - Germany, London - United Kingdom, Mumbai - India, Muscat - Oman, Paris - France, Sydney - Australia, Vinhedo - Brazil. See Global data centers.
- Added support for Fortinet security PoPs: Auckland - New Zealand. See Global data centers.
- Updated support for Fortinet security PoPs: London - United Kingdom, Komagome - Japan. See Global data centers.

What's new for 25.4.124 (25.4.c.1 Feature)

25.4.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 50.

What's new for 25.4.109 (25.4.c Feature)

- For new instances, support has been added for FortiClient 7.4.5 for FortiSASE desktop users. The transition path for existing customers is not yet available and will be expected in an upcoming release. See Supported FortiClient 7.4.7 features on page 29.
- For existing instances, 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 Supported FortiClient 7.2.14 features on page 34.

- For new instances supporting FortiClient 7.4, where security posture tags and tagging rules can be created and managed together in the combined *Tagging rules* tab in *Endpoint management > Security Posture* tags. The transition path for existing customers is not yet available and will be expected in an upcoming release. See Security posture tags and tagging rules.
- For new instances, as a remote user connectivity alternative when standard IPsec ports over UDP are blocked by networks, added support for IPsec over TCP with TCP port 443. This feature requires Windows or Mac endpoints running FortiClient 7.4.5 or later. See Global connection settings.
- For new instances, added support for configuring DNS suffixes for IPsec tunnels in an endpoint profile under *Connection > Advanced Settings*. DNS suffixes are used for resolving short hostnames and are appended to subdomains. Also, DNS resolutions of endpoints apply the DNS suffixes in the order they are configured. Whenever a DNS suffix is configured or modified, users must reconnect the agent tunnel for changes to take effect. This feature requires Windows endpoints running FortiClient 7.4.5 or later. See Advanced settings.
- For new instances, added a new rule type for security posture tagging based on CrowdStrike ZTA scores, which are generated by the CrowdStrike Falcon sensor, reflecting the endpoint's security posture. This feature requires Windows and Mac endpoints running FortiClient 7.4.5 or later. See Tagging rule types.
- For new instances, added support for ZTNA automatic login using OAuth, which allows Windows users signed in to their workstations, joined to a Microsoft Entra ID domain, to be automatically allowed access to ZTNA-protected TCP resources by using the same login information. This feature requires valid supporting Entra ID configuration, Windows endpoints running FortiClient 7.4.5 or later, and FortiGate devices acting as a ZTNA application gateways running FortiOS 7.6.1 or later. See ZTNA.
- For new instances, FortiSASE can now learn security posture tags directly from FortiClient when using ZTNA application gateway sharing. By enabling *Record client tags and information* in the *Endpoint management > Security posture tags > Settings* tab, the security posture tag timeout can be defined in FortiSASE. This feature requires FortiClient 7.4.5 and later. See Endpoint management settings.
- Added System for Cross-domain Identity Management (SCIM) support for automated user provisioning from Entra ID, FortiAuthenticator, and Okta SAML IdPs. The SCIM client (IdP) sends user and group information to the SCIM server (FortiSASE as SP). This is a select availability feature that requires a Fortinet Support ticket to enable on new and existing instances. See SCIM server support.
- Added support for configuring and matching geography addresses as the source in policies which allow specific security profiles to be applied to remote user agents connecting from specific geolocations. See Configuring a geography-based policy.
- For MSSPs, added central management support for synchronizing multiple tenants' FortiSASE instances from a single FortiManager instance or from multiple FortiManager instances.
  - Currently, each ADOM in FortiManager supports synchronizing configuration with a single FortiSASE instance.
  - A FortiManager key, if configured, allows a FortiManager appliance registered under a FortiCare account belonging to a parent Organization Unit (OU) to manage the FortiSASE tenant.
  - The FortiManager key can be revoked to only allow connections from FortiManager appliances registered to the current FortiCare account and disable connections from parent OU FortiManagers.
  - The FortiManager key will be strictly matched and must match in both FortiManager and FortiSASE connector settings. If a key is revoked on the FortiSASE tenant, then the key must also be removed on the FortiManager intending to manage the tenant.
  - Central management is still a select availability feature that requires a Fortinet Support ticket to enable on new and existing instances.

  See Central management for MSSP tenants.

- Extended existing REST API support to include retrieval of data transfer statistics for FortiSASE instances, including annual allotment, consumed bytes, and consumption percentage. See Appendix B - REST API.
- Added support for Public Cloud security PoPs: Bangkok - Thailand, Cyberjaya - Malaysia, Columbus - Ohio - USA, Montreal - Canada, Moncks Corner - South Carolina - USA, Tokyo - Japan. See Global data centers.

What's new for 25.4.96 (25.4.b.2 Feature)

25.4.b.2 is a maintenance release. For a list of resolved issues, see Resolved issues on page 50.

What's new for 25.4.88 (25.4.b.1 Feature)

25.4.b.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 50.

What's new for 25.4.78 (25.4.b Feature)

- For greater performance and security, FortiSASE Cloud Security tunnel will be migrating from SSL to IPsec starting early 2027. FortiSASE Cloud Security tunnel will support a hybrid IPsec/SSL mode during the transition period that is available as an opt-in feature for SSL VPN instances through the *Operations > Administration > Software audit & version* page's best practices. This allows customers time to verify client-side changes for IPsec mode before migrating with confidence. See Hybrid IPsec/SSL mode.
- Added support for configuring authenticated onboarding with Entra ID for SAML SSO using an existing Entra ID domain, which allows an endpoint profile configured with a matching AD group from the domain to be assigned to matching endpoints with users authenticated using an Entra ID account. Authenticated onboarding is still a select availability feature. See Authenticated onboarding.
- Simplified pre-logon tunnels such that endpoints establish tunnels with the nearest FortiSASE Security PoP using certificate-based authentication. This simplified approach supports a shared policy to allow destinations and requires configuring an SPA hub with connectivity to an Active Directory server. For instances with existing pre-logon tunnels configured, the previous approach is still supported and only the simplified approach is supported going forward after disabling existing pre-logon tunnels in all endpoint profiles. See Pre-logon tunnel.
- Added support for configuring the FortiClient built-in browser used for SAML SSO authentication in an endpoint profile under *Connection > Tunnel settings*. See Tunnel settings.
- 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 SAML single signout in the agentless ZTNA bookmark portal. See Accessing the bookmark portal.
- Added support for configuring one-time schedules with policies and proxy policies. See Schedules.
- For existing instances, support has been added for a new endpoint vulnerability report based on logs collected from FortiClient endpoints. See Report types.
- For existing 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 existing 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.
- For existing 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.
- Added support for performing a factory reset on a FortiSASE instance that returns it to its initial provision point, disconnects all users, and deregisters all endpoints.
  - This feature includes options to keep the dedicated public IP addresses or to repick PoP locations (you can only choose one option and they cannot be used together).
  - After accepting the acknowledgment, an email with a passcode is sent to the email address for the instance's primary FortiCloud account, and after entering the passcode, the reset will begin.
  - Currently, this feature is enabled by default for FortiSASE instances with the Not-for-Resale (NFR) and Advanced NFR licenses applied.
  - For FortiSASE instances with other licenses applied, this is a select availability feature requiring a FortiCare Support ticket.
  - This feature is available only when logged into the FortiSASE portal with the principal FortiCloud account, where an OTP code is sent via email. This feature is not available from IAM accounts.

  See Factory reset.
- Enhanced endpoint upgrade rule page to more clearly indicate the option to defer a FortiClient installation and to indicate that once the installation starts, the endpoint will automatically reboot upon completion. See Endpoint upgrade.
- Simplify security PoP selection for Advanced and Comprehensive customers to show all available locations in one page. See Provisioning.
- Added support for Public Cloud security PoPs: Dubai - United Arab Emirates, Frankfurt - Germany, Miami – USA, Paris - France, Toronto - Canada. See Global data centers.
- Updated support for Fortinet security PoPs: Ashburn - Virginia - USA. See Global data centers.
- Support has been added to view the FortiSASE portal in French. See Language support on page 48.
- Support has been added to view the FortiSASE portal in Japanese. See Language support on page 48.

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

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

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

25.3.c.1 is a maintenance release. For a list of resolved issues, see Resolved issues on page 50.

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 28.
- 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 50.

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 on page 43.
- Added support for simplified branch on-ramp licensing. See SIA for Branch On-ramp site-based remote users on page 43.

    - 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 on page 43.
- 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 in policy packages 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 50.

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 50.

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 50.

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 28.
- 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 50.

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 50.

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 28.
- 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, 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 50.

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 50.

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 50.

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 28.
- 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 28.
- 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 42.
- 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 50.

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 50.

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

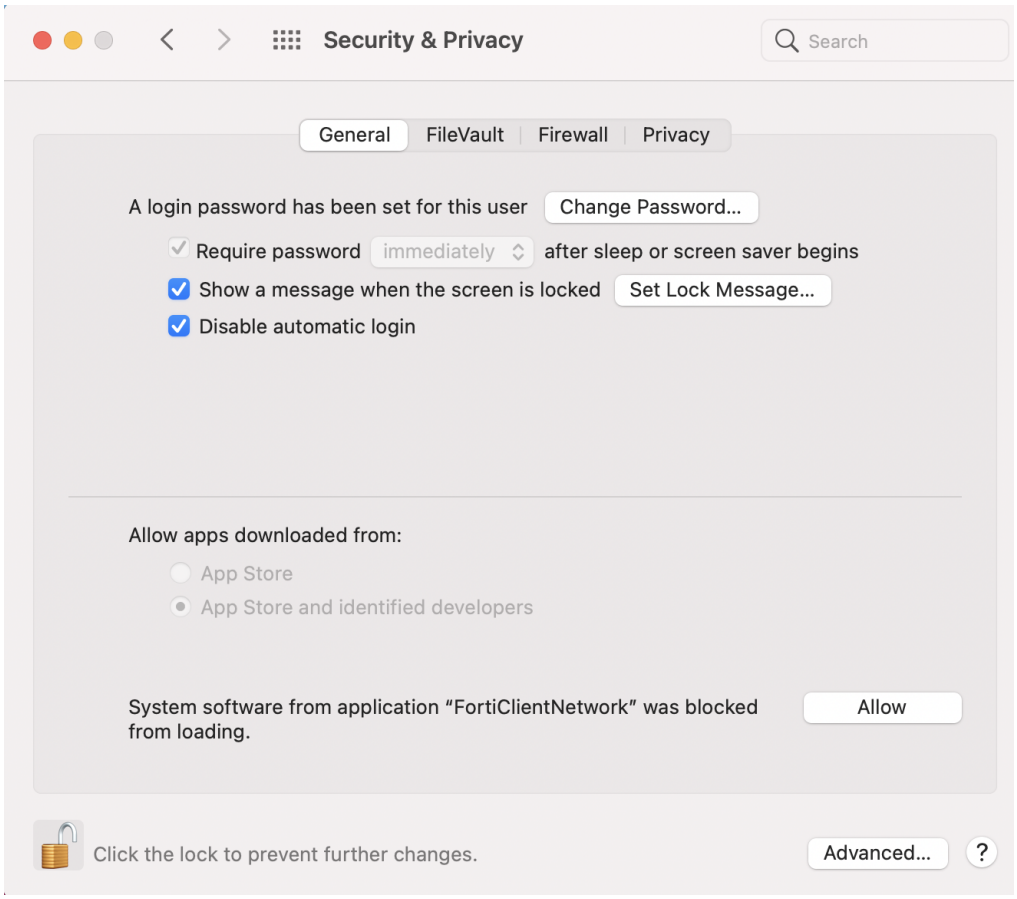
The *Profile > Removable Media Access Control* option only works if you enable Malware Protection, an optional feature, when installing FortiClient on the endpoint.

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) 7.4.7
- FortiClient (macOS) 7.4.7
- FortiClient (Windows) 7.2.14
- FortiClient (macOS) 7.2.14
- FortiClient (Android)
- FortiClient (iOS)

The recommended version for FortiSASE for desktop users is dependent on your instance status:

- For new instances created in FortiSASE Feature 25.4.c or later, FortiClient 7.4.7 is the recommended version for FortiSASE for desktop users.
- For existing instances created before FortiSASE Feature 25.4.c, FortiClient 7.2.14 is the recommended version for FortiSASE for desktop users.

FortiSASE has updated installers and download links to use FortiClient 7.4.7 and 7.2.14, respectively.

- 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 and 7.4.

Considerations

- For existing instances created before 24.4.b.1 with remote user connectivity to FortiSASE using SSL, the recommended version is FortiClient 7.2.14.
- Starting in FortiSASE 24.4.b.1, IPsec remote agent support is enabled by default on new instances.
  - For new instances with IPsec remote user support enabled, the recommended version is FortiClient 7.4.7.
  - For existing instances created before 25.4.b with IPsec remote user support enabled, the recommended version is FortiClient 7.2.14.
  - 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.
- For new instances created in FortiSASE Feature 25.4.b or later, the MSI version of the FortiClient installer is not available.

Third party software

- FortiSASE is validated against operating systems within their vendor's standard support lifecycle. Platforms at or beyond End of Life, End of Extended Support, or maintained only through paid extended support agreements may experience degraded performance or incompatibility with FortiClient and FortiSASE components.
- Fortinet cannot guarantee performance or commit engineering resources to resolve issues on legacy operating systems. Customers experiencing issues on such platforms are encouraged to migrate to a supported OS version.

This section includes the following information:

Supported FortiClient 7.4.7 features

This topic includes information on the following platforms:

Windows

The following table lists the FortiClient version 7.4.7 supported features for the Windows platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Diagnostic logs on-demand	✓	✓

Feature	IPsec	SSL VPN
Digital experience monitoring agent	✓	✓
FortiGuard Forensics Analysis	✓	✓
FSSOMA connectivity status	✓	✓
Access		
Microsoft Entra ID options		✓
Autoconnect using SAML SSO	✓	✓
Steering bypass destinations	✓	✓
Exempt autoconnect via DNS server	✓	✓
Exempt autoconnect via DHCP server	✓	✓
Exempt autoconnect via local subnet	✓	✓
Exempt autoconnect via ping server	✓	✓
Exempt autoconnect via public IP	✓	✓
Configurable MTU on IPsec	✓	
Endpoint profile assignment (Entra ID Groups)	✓	✓
Endpoint profile change notifications	✓	✓
Endpoint telemetry	✓	✓
Tunnel connectivity notifications	✓	✓
Tunnel disconnect from FortiSASE	✓	✓
External browser for SAML login	✓	✓
SAML engine for built-in browser	✓	✓
Force always-on tunnel	✓	✓
Network lockdown	✓	✓
Pre-logon tunnel	✓	✓
Security posture tags	✓	✓
Split DNS/DNS redirection	✓	✓
SSL tunnel remains active when idle		✓
SSL tunnel DTLS support		✓
SSL tunnel to FortiSASE		✓
FSSO		
FortiClient SSO Mobility Agent	✓	✓

Feature	IPsec	SSL VPN
Protection		
Anti-ransomware	✓	✓
Next-generation AntiVirus	✓	✓
Removable media access control	✓	✓
Media block notifications	✓	✓
Vulnerability scan	✓	✓
Event-based vulnerability scan	✓	✓
Sandboxing (Cloud + on-prem)	✓	✓
ZTNA		
Security posture tagging rules	✓	✓
ZTNA remote access	✓	✓
ZTNA JWT authentication	✓	✓
VPN Enhancements		
IPsec over TCP	✓	
IPsec transparent reconnect	✓	

macOS

The following table lists the FortiClient version 7.4.7 supported features for the macOS platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Diagnostic logs on-demand	✓	✓
Digital experience monitoring agent	✓	✓
FortiGuard Forensics Analysis		
FSSOMA connectivity status	✓	✓
Access		
Microsoft Entra ID options		
Autoconnect using SAML SSO	✓	✓
Steering bypass destinations	Only subnet	Only subnet
Exempt autoconnect via DNS server	✓	✓
Exempt autoconnect via DHCP server	✓	✓

Feature	IPsec	SSL VPN
Exempt autoconnect via local subnet	✓	✓
Exempt autoconnect via ping server	✓	✓
Exempt autoconnect via public IP	✓	✓
Configurable MTU on IPsec	✓	
Endpoint profile assignment (Entra ID Groups)	✓	✓
Endpoint profile change notifications	✓	✓
Endpoint telemetry	✓	✓
Tunnel connectivity notifications	✓	✓
Tunnel disconnect from FortiSASE	✓	✓
External browser for SAML login	✓	✓
SAML engine for built-in browser	✓	✓
Force always-on tunnel	✓	✓
Network lockdown	✓	✓
Pre-logon tunnel		
Security posture tags	✓	✓
Split DNS/DNS redirection	✓	✓
SSL tunnel remains active when idle		✓
SSL tunnel DTLS support		✓
SSL tunnel to FortiSASE		✓
FSSO		
FortiClient SSO Mobility Agent	✓	✓
Protection		
Anti-ransomware		
Next-generation AntiVirus	✓	✓
Removable media access control	✓	✓
Media block notifications	✓	✓
Vulnerability scan	✓	✓
Event-based vulnerability scan	✓	✓
Sandboxing (Cloud + on-prem)	✓	✓
ZTNA		

Feature	IPsec	SSL VPN
Security posture tagging rules	✓	✓
ZTNA remote access	✓	✓
ZTNA JWT authentication	✓	✓
VPN Enhancements		
IPsec over TCP	✓	
IPsec transparent reconnect	✓	

Android

The following table lists the latest FortiClient version supported features for the Android platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Access		
Autoconnect using SAML SSO		✓
Endpoint telemetry	✓	✓
External browser for SAML login	✓	✓
SSL tunnel remains active when idle		✓
SSL tunnel DTLS support		✓
SSL tunnel to FortiSASE		✓
Protection		
Vulnerability scan	✓	✓
Sandboxing (Cloud + on-prem)	On-prem only	On-prem only
ZTNA		
Security posture tagging rules		✓

iOS

The following table lists the latest FortiClient version supported features for the iOS platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Access		

Feature	IPsec	SSL VPN
Autoconnect using SAML SSO		✓
Endpoint telemetry	✓	✓
External browser for SAML login	✓	✓
IPsec IKEv2 + PSK + SAML	✓	
IPsec IKEv2 + PSk + Local user	✓	
Force always-on tunnel		✓ MDM is required
Pre-logon tunnel		✓ MDM is required
SSL tunnel remains active when idle		✓
SSL tunnel DTLS support		✓
SSL tunnel to FortiSASE		✓
ZTNA		
Security posture tagging rules		✓

Supported FortiClient 7.2.14 features

This topic includes information on the following platforms:

Windows

The following table lists the FortiClient version 7.2.14 supported features for the Windows platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Diagnostic logs on-demand requests from FortiSASE	✓	✓
Digital experience monitoring agent*	✓	✓
FortiGuard Forensics Analysis*	✓	✓
Access		

Feature	IPsec	SSL VPN
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	✓	✓
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	✓	✓
IPsec VPN to FortiSASE using IKEv2, Preshared Key, and SAML	✓	
IPsec VPN to FortiSASE using IKEv2, Preshared Key, and Local user	✓	

Feature	IPsec	SSL VPN
Network lockdown	✓	
Pre-logon tunnel	✓	✓
Show security posture tags on FortiClient	✓	✓
Split DNS or DNS redirection	✓	✓
SSL tunnel connection remains active after endpoint has been idle		✓
SSL tunnel support for DTLS		✓
SSL tunnel to FortiSASE		✓
FSSO		
FortiClient SSO mobility agent	✓	✓
Protection		
Antiransomware	✓	✓
Next generation antivirus (AV) – real-time AV and cloud malware protection	✓	✓
Removable media access control	✓	✓
Removable media access control – notify endpoint of blocks		
Vulnerability scan	✓	✓
Vulnerability scan - event-based scan	✓	✓
Sandbox		
Sandboxing - on-premise and FortiSASE Cloud Sandbox	✓	✓
ZTNA		
Security posture tagging rules	✓	✓
ZTNA remote access	✓	✓

* Requires Advanced or Comprehensive subscription.

macOS

The following table lists the FortiClient version 7.2.14 supported features for the macOS platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	IPsec	SSL VPN
Digital experience monitoring agent*	✓	✓
Access		
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓	✓
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	✓	✓
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 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	✓	✓
IPsec VPN to FortiSASE using IKEv2, Preshared Key, and SAML	✓	
IPsec VPN to FortiSASE using IKEv2, Preshared Key, and Local user	✓	
Network lockdown	✓	
Show security posture tags on FortiClient	✓	✓
Split DNS or DNS redirection	✓	✓

Feature	IPsec	SSL VPN
SSL tunnel connection remains active after endpoint has been idle		✓
SSL tunnel support for DTLS		✓
SSL tunnel to FortiSASE		✓
FSSO		
FortiClient SSO mobility agent	✓	✓
Protection		
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 (macOS) 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	✓	✓
ZTNA		
Security posture tagging rules	✓	✓
ZTNA remote access	✓	✓

* Requires Advanced or Comprehensive subscription.

Android

The following table lists the FortiClient version supported features for the Android platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	SSL VPN
Access	
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓

Feature	SSL VPN
Endpoint telemetry	✓
External browser as user-agent for SAML login	✓
Force always on tunnel	✓
Show security posture tags on FortiClient	✓
SSL tunnel support for DTLS	✓
SSL tunnel to FortiSASE	✓
Sandbox	
Sandboxing (On-premise and FortiSASE Cloud Sandbox)	On-premise only
ZTNA	
Security posture tagging rules	✓

iOS

The following table lists the FortiClient version supported features for the iOS platform for IPsec and SSL VPN tunneling. Likewise, the table lists feature support by the FortiSASE portal:

Feature	SSL VPN
Access	
Autoconnect to FortiSASE using SAML single sign on (SSO)	✓
Endpoint telemetry	✓
External browser as user-agent for SAML login	✓
Force always on tunnel	✓ 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	
Show security posture tags on FortiClient	✓
SSL tunnel support for DTLS	✓

Feature	SSL VPN
SSL tunnel to FortiSASE	✓
ZTNA	
Security posture tagging rules	✓

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 41	Secure access to the internet using FortiClient agent.
SIA for FortiExtender site-based remote users on page 41	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 42	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 42	Secure access to the internet using FortiAP device as FortiSASE edge device.
SIA for Branch On-ramp site-based remote users on page 43	Secure access to the internet using an IPsec device acting as an on-ramp to FortiSASE.
Log forwarding on page 43	Forward logs to an external server, such as FortiAnalyzer.
Central management using FortiManager on page 44	Centrally manage FortiSASE configuration settings from FortiManager
RBI on page 44	For proxy users, isolate browser sessions of certain websites or categories in an isolated environment, which renders content safely in a remote container.
Secure Browser on page 44	Integrated management of the FortiSASE Secure Browser extension. Administrators can gain full visibility into browser activity without deep inspection, can monitor and block web-based threats, and can prevent data exfiltration.
ZTNA on page 45	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases.

Use case	Description
SPA using a FortiGate SD-WAN hub on page 45	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network.
SPA using a FortiSASE SPA hub on page 46	Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW).
SPA using FortiGate SD-WAN Service Bundle subscription on page 46	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 47	Access to private company-hosted applications behind the FortiGate NGFW using Fabric Overlay Orchestrator.
SPA for an MSSP hub on page 48	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 48	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.

> Topics referencing FortiExtender in the FortiSASE Administration Guide also apply to FortiBranchSASE.

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 50 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
- 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.
- Support of central management for MSSP tenants requires FortiManager 7.4.9 or later, or FortiManager 7.6.5 or later.
- 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
- A yearly isolation data limit, enforced at the instance level, is 1.2 GB per user included per year. Beyond that limit, all users' isolation traffic will be blocked.
  - For example, for an instance with 50 users, the yearly isolation data limit that is enforced on the instance is 60 GB per year.
  - If the cumulative isolation traffic of these 50 users exceeds 60 GB at any time in the year, then isolation traffic for all 50 users in that instance will be blocked.

Secure Browser

- If the Secure Browser extension has already been deployed on endpoints as part of *FortiMail Workspace Security*, specifically, *FortiMail Browser Security* support, then the administrator should not enable Secure Browser in FortiSASE.
- FortiSASE Secure Browser requires a FortiSASE instance with an Advanced or Comprehensive remote users FortiSASE subscription.
- Currently, the FortiSASE Secure Browser extension is supported in Windows and MacOS on Google Chrome and Microsoft Edge web browsers.
- SAML SSO users must be integrated with FortiSASE Secure Browser before the feature can be configured and deployed. Therefore, this feature requires access to a SAML SSO IdP such as Entra ID.

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

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.

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 48.

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 45.

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 • 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 recommended templates for SD-WAN overlays • 7.4.0 or later • 7.6.0 or later
FortiClient	• 7.2.14 for existing instances created before 25.4.c • 7.4.7 for new instances in 25.4.c or later

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 45.

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	• 7.2.14 for existing instances created before 25.4.c • 7.4.7 for new instances in 25.4.c or later

SPA using FortiGate SD-WAN Service Bundle subscription

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

The FortiGate SD-WAN Service Bundle subscription is available for FortiGate F-series hardware models starting from 100F and above, and 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 SD-WAN Service Bundle includes the following FortiSASE subscriptions:

- 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) depend on the model of F-series FortiGate or G-series FortiGate licensed, outlined as follows:

Model	Included remote user seats for each model	Number of security PoPs available
Below 100F Below 120G	None	N/A
100F to 600F 120G to 600G	10	2
1000F 700G to 1500G	50	2 to 4
1800F and above 1800G and above	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 SD-WAN Service Bundle subscription applied under the same FortiCloud account as FortiSASE. For example, consider that a customer purchases the FortiGate SD-WAN Service 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 45.

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	• 7.2.14 for existing instances created before 25.4.c • 7.4.7 for new instances in 25.4.c or later

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

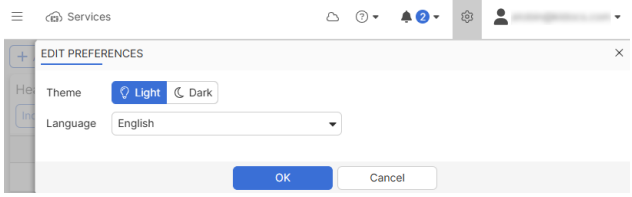
The following languages are supported for the FortiSASE Feature portal:

- English
- Japanese (日本語)

- French (Français)

To select the portal language:

1. Select the gear icon from the FortiSASE banner. The *Edit Preferences* pane is displayed.



> In the *Edit Preferences* pane, select a *Theme* to switch between *Light* and *Dark* mode.

2. Select the desired *Language* from the dropdown list.
3. Click *OK*. The portal will display in the selected language.

Resolved issues

The following issues have been fixed in version 26.1.107 Feature unless noted otherwise. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
1141062	External feeds not working with private domain behind SPA hub configured with BGP on loopback.
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.
1205320	Client does not receive an IP address via DHCP when connected to FortiGate as FortiSASE LAN extension.
1205675	FSSO not working with FortiAuthenticator behind SPA hub configured with BGP on loopback.
1206424	In *Video Filter* profile, channel filter is being overridden by FortiGuard category rule.
1245592	Allow standard license instances to enable SCIM feature.
1248163	After migration of SSL VPN instances with DNS configuration of VPN DNS server differing from SWG and Edge device DNS server, DNS uses DNS over TLS (DOT) instead of DNS over UDP protocol.
1253976	Admin cannot delete an unused Security Posture tag.
1257261	Custom FortiExtender and LAN Extension control plane subnet overwritten back to default of 10.252.0.0/16 when BGP configuration is saved.
1258866	SaaS monitoring tab fails to load for instances monitoring Google.Docs (docs.google.com) due to an unexpected occurrence of false positive DEM health events for this SaaS application.
1259603	Admin cannot view more than 50 Security Posture tags.
1265187	Fixed issue with custom tunnel missing gateway information.
1269965	Users field in private access policy ID 1000 does not show all the users and user groups configuration. Enable the *ID* column to easily locate this policy.
1273604	Intermittent HTTP 303 Redirect Loop with Proxy/SWG and SSO configured.
1273643	Admin cannot save changes to FortiBranch device profile.
1275765	Log forwarding not working in instances provisioned for designated Public Cloud locations whose naming convention includes *-O*.
1277893	For existing instances supporting FortiClient 7.2, when creating an endpoint profile with SSO enabled, the SAML port is not specified causing FortiClient 7.4 endpoints to be unable to establish agent tunnels.

Bug ID	Description
1278281	Fixed issue with Entra ID domain synchronization.
1286095	Fixed an issue that prevented supported configuration objects from being synchronized from FortiManager to FortiSASE for central management.
1287036	Unable to view the IPsec Custom Tunnel in FortiSASE portal when custom tunnel uses Secure Internet Access in the name.
1288428	Fixed issue re-registration process for endpoints.
1290465	Fixed issue where large number of endpoints became unlicensed and were missing endpoint profile features.

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

Bug ID	Description
1267769	Proxy/SWG SSO SAML authentication failure due to *.*fortisase.com* in PAC. **Workaround**: Perform these steps: **1.** Clone the PAC file to a custom PAC. **2.** Remove *.*fortisase.com* from the new PAC file. **3.** Make sure turbo domain being used for both Proxy and SAML are the same. **4.** Deploy the PAC file to small group for testing. Once confirmed the workaround fixes the issue, deploy the PAC file to other endpoints.
1285584	FortiClient 7.2 and 7.4 vulnerability scan detects embedded Python application of DEM agent as a vulnerable 3rd Party App. **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 26.1.107 Feature. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
716833	FortiClient (macOS) does not support application-based split tunnel.
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

Bug ID	Description
	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)
1179359	API-based CASB region selection does not display *Europe* region in dropdown selection.
1196263	Failed to upgrade edge device FortiAP 431F/231F firmware version from 7.2 to 7.4.
1205444	Unable to configure Agentless ZTNA on an Advanced license instance despite having a dedicated IP already assigned.
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. **Workaround**: After the migration, reconfigure scheduled reports and email groups, if needed.
1261507	Video filter does not block streaming of matching videos when either the default action for all categories or the action for a specific FortiGuard category is configured to block.
1263849	FortiAuthenticator Cloud cannot learn and synchronize FortiSASE certificates for SCIM integration. **Workaround**: Under Trusted CA section of FortiAuthenticator Cloud, import any intermediate CA certificates in the certificate chain. Use an online SSL server test to determine the certificate chain.
1267266	*Auto* option for FortiSASE Cloud Security Tunnel encapsulation not working since initial IKE negotiation over UDP works fine but ISP blocks UDP ports 500/4500 so fail back to TCP never occurs. Currently, the administrator cannot enforce IPsec over TCP via endpoint profile. **Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance.
1269534	DEM agent TCP latency feature showing incorrect results. **Workaround**: Open a new FortiCare Support ticket to implement a workaround for your FortiSASE instance.
1274013	In the *Protection* tab of an endpoint profile, folders/files defined in *Exclude specified folders/files* are not being excluded from Next Generation Antivirus scans.

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)

- 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.
- 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 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 FortiSASE Sandbox in an endpoint profile, to ensure sandbox functionality, the connection to the Fortinet-FortiSandbox infrastructure destination must be allowed in an agent tunnel policy in the following cases:
  - When the Allow-All agent tunnel policy has been disabled or deleted.
  - When any other agent tunnel policy with *All internet Traffic* as the destination and *Service* set to *ALL* is not present.

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.
- Currently, FortiSASE only supports establishing an FSSO connection to a private FortiAuthenticator behind an SPA hub configured for BGP per overlay.
- Agentless RBI does not work when SWG SSO is configured.
  - **Workaround**: Ensure the security profile group used for the "CSP_REPORT" proxy policy is using certificate inspection instead of deep inspection.

DNS

- *Failed to update DNS rule* error caused by overlapping backend operations is observed when viewing *Network > DNS* page immediately after saving a DNS rule with a large number of domains.
  - **Workaround**: After saving a DNS rule, wait some time before accessing the *Network > DNS* page. Consider configuring domains into multiple DNS rules, ideally less than 10 domains per DNS rule, instead of configuring all domains into a single DNS rule.

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.

Proxy

- Proxy mode is not supported on iOS devices.
- To ensure Proxy/SWG users can properly authenticate using SAML SSO, administrators must not use the `dnsResolve()` function in custom PAC files.

www.fortinet.com