Release Notes

FortiSASE 24.1.56

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

April 17, 2024
FortiSASE 24.1.56 Release Notes
72-24156-1012638-20240417

TABLE OF CONTENTS

Change log 4
Introduction 5
What's new 6
What's new for 24.1.56 (24.1.c) 6
What's new for 24.1.37 (24.1.b) 7
What's new for 24.1.10 (24.1.a) 8
What's new for 23.4.49 (23.4.b) 9
What's new for 23.4.31 (23.4.a) 10
Special notices 11
Removable media access 11
Activating the FortiClientNetwork extension 11
Select availability features 13
Product integration and support 14
Supported FortiClient features 14
Common use cases 16
SIA for FortiClient agent-based remote users 17
SIA for FortiExtender site-based remote users 17
SIA for FortiGate SD-WAN secure edge site-based remote users 18
SIA for FortiAP site-based remote users 18
Log forwarding 18
ZTNA 18
SPA 19
SPA Service Connection license 19
SPA FortiCloud account prerequisites 19
SPA using a FortiGate SD-WAN hub 19
SPA using a FortiSASE SPA hub 20
SPA using a FortiSASE SPA hub with Fabric overlay orchestrator 20
Resolved issues 21
Known issues 22
Limitations 23
FortiClient desktop (Windows, macOS, Linux) 23
FortiClient Android 23
FortiClient Cloud 23
Authentication 23
FortiSandbox 23

Change log

Date	Change description
2024-04-11	Initial release.
2024-04-12	Added Select availability features on page 13. Updated Known issues on page 22.
2024-04-15	Updated build # to 24.1.55.
2024-04-17	Updated build # to 24.1.56. Updated Resolved issues on page 21.

Introduction

This document provides a list of new features and changes and known issues for FortiSASE 24.1.56. Review all sections of this document before using this service.

What's new

- What's new for 24.1.56 (24.1.c) on page 6
- What's new for 24.1.37 (24.1.b) on page 7
- What's new for 24.1.10 (24.1.a) on page 8
- What's new for 23.4.49 (23.4.b) on page 9
- What's new for 23.4.31 (23.4.a) on page 10

What's new for 24.1.56 (24.1.c)

- All FortiSASE instances have log retention enabled with a log retention period of 30 days by default. See Log retention policy.
- Added support for provisioning FortiSASE instances with fewer security PoPs, removing the previous restriction to select four security PoPs. Also, FortiSASE administrators can add more security PoPs after initial provisioning if fewer security PoPs have been allocated than the entitled maximum number of security PoPs. See Appendix A - FortiSASE data centers.
- Added support for the FortiSASE Region Add-on license. Once the license has been applied, FortiSASE administrators can select extra security PoPs after logging into the FortiSASE portal. See Appendix A - FortiSASE data centers.
- The configuration of SSO on FortiSASE now supports Active Directory Federation Services (AD FS). With this support FortiSASE administrators can import and use a custom Service Provider (SP) certificate of their choice or select in-built *FortiSASE Default Certificate* inside the SSO configuration. The custom or in-built SSO certificate can then be imported into the required Identity Provider for SP verification. The feature now also supports SHA-256 for signing SAML Authentication Requests. See Configuring FortiSASE with AD FS SSO.
- The feature allows FortiSASE administrator to group non-AD endpoints in a nested group structure and assign the configured nested group to a custom endpoint profile. Endpoint profiles assigned to the non-AD endpoints can be viewed from Profile column under *Network > Managed Endpoints*. See Groups & AD Users.
- Added support for configuring Custom IPS signatures and applying it in Custom IPS Rules inside Intrusion Prevention Security profile. This feature also adds concept of Profile resources that enables central configuration and sharing of Custom IPS Signatures, FortiGuard categories, and Custom Web Filter categories across different security profiles. See Intrusion prevention.
- FortiSASE now supports configuration of custom IPsec and SSL VPNs (also called as *Alternative VPN*) in the endpoint profiles. These custom VPNs are typically useful for users or endpoints that require VPN connection to on-prem FortiGate or VPN gateways. Endpoints with the custom VPN endpoint profiles would need to manually re-connect to FortiSASE VPN if it's used as a backup VPN connection. See Connection.
- Added support for requesting FortiClient diagnostic logs on-demand from a single online Windows endpoint from either the *Details* tab in *View Endpoint Details* or from *More options* in the *Endpoints* tab in the *Managed Endpoints* page. Once the endpoint receives the log request, log collection will take place in the background. This process takes approximately 20 minutes. When new logs are generated, then the old ones will be overwritten. See Requesting FortiClient diagnostic logs from endpoints.
- Added support for resource-based access control in FortiSASE by showing or hiding GUI features based on the Read-Only, Read & Write, or No Access permissions assigned to IAM users using the FortiCare IAM management portal. See Configuration workflow. Access control of the following resources has been added:

  - User & Authentication
  - Policy
  - Logging
  - Monitoring
  - Dashboards
  - Network
  - System
  - Security
  - Endpoint Management
  - Infrastructure
- Added support in FortiSASE DLP for managing access to files with Microsoft Purview Information Protection (MPIP) sensitivity labels applied. MPIP sensitivity labels are created in a Microsoft portal and applied to files using Office 365 applications. The Globally Unique Identifier (GUID) of an MPIP sensitivity label is configured and selected in a DLP rule with the *Data Source Type* of *MPIP Label*. See Blocking file with MPIP sensitivity label example.
- Enhancement to FortiSASE portal's user interface through optimizations to backend services for seamless user experience.
- Enhancements made to FortiSASE's backend to optimize auto-connect feature.
- Added datacenter support for additional Public Cloud Locations:
  - Johannesburg, South Africa
  - Sao Paulo, Brazil

  See Global data centers.

What's new for 24.1.37 (24.1.b)

- For new instances, added support for unique SSL VPN IP address ranges per FortiSASE security PoP within the overall 100.65.0.0/16 range. Previously, SSL VPN IP address ranges were not unique between security PoPs. Also, for new instances added support for removing source NAT (SNAT) for remote VPN user traffic destined for secure private access (SPA) hubs. By default, FortiSASE performs SNAT for such traffic. On new instances, both features are enabled together and allow administrators to identify remote VPN users accessing private resources that SPA hubs protect. See Remote VPN user identification.
- For new instances, added support for FortiClient variations based on the FortiSASE remote users license type. Instances with a Standard remote users FortiSASE license use the standard FortiClient installer. Instances with an Advanced or a Comprehensive remote users FortiSASE license use the FortiClient installer with the digital experience monitoring (DEM) agent. See Digital Experience.
- DEM provides granular and real-time information regarding endpoint health by employing a DEM agent installed on endpoints. You can monitor information such has CPU, memory, hard drive, and network usage in real time. It can also trace network performance from an endpoint to various SaaS providers, thus providing end-to-end network visibility and performance insights. To use DEM, FortiSASE requires an Advanced or a Comprehensive remote user license. See Digital Experience.
- Expanded REST API support with resource API v2 for managing additional network and security configuration settings:
  - Antivirus file types
  - Applications and application categories
  - DNS and implicit DNS rules
  - FortiGuard categories and FortiGuard local categories
  - Geography address countries

    - Hosts and host groups
    - Services, service groups, service categories
    - Wildcard FQDNs custom

  See Appendix C - REST API.
- Added support for configuration and use of custom DNS servers that VPN, secure web gateway (SWG), and Thin Edge users use. You can configure custom DNS servers inside the implicit DNS rules for these user types. See DNS Settings.
- Added support for creating external threat feeds of types such as threat hosts, DNS filter domains, and web filter FQDNs. After creation, you can use the external threat feeds inside the *Destination address* field in a secure Internet access (VPN/SWG) and/or private access policy and in the web filter and/or the DNS filter to restrict/allow access accordingly. See Feeds.
- Added support for exporting endpoint details such as device name, OS version, FortiClient version, and endpoint groups in a CSV file. You can perform the export operation from *Network* > *Managed Endpoints* using *Export All*. See Managed Endpoints.

What's new for 24.1.10 (24.1.a)

- Added support within the managed security services provider (MSSP) portal for organizational unit administrators other than the primary account to provision tenant accounts associated with placeholder member accounts. See Configuration workflow.
- Added support for configuring Sonoma as a macOS version in ZTNA tagging rules. See Tagging rule types.
- FortiSASE instances with an Advanced or a Comprehensive remote users FortiSASE license include an embedded onboarding guide that is displayed upon first login. This guide contains instructions and videos that streamline initial configurations for the secure Internet access (SIA) endpoint use case. The information presented may not apply to instances with existing configurations. When skipped, the guide can be accessed later from the *Help* dropdown in the app header. See Embedded onboarding guide.
- Added support for requesting a new FortiGuard Forensics Analysis for a suspicious endpoint and viewing a summary of analysis requests from the *Managed Endpoints* page. After a forensics analyst completes the analysis within five business days, the verdict along with a downloadable report are updated in FortiSASE. You can have a maximum of five forensic analysis requests in progress at a given time. This feature requires either an Advanced or a Comprehensive remote users FortiSASE license. See FortiGuard Forensics Analysis.
- Added support for configuring FortiSASE data loss prevention (DLP) from within the DLP widget in *Configuration* > *Security*. DLP prevents sensitive data from leaving or entering your network. DLP requires enabling SSL deep inspection to decrypt and inspect content in encrypted traffic. See DLP.
- Added support for a new generated Shadow IT report under the *Applications* section within *Analytics* > *Scheduled Reports*. This report summarizes the usage of SaaS applications compared to all applications, sanctioned versus unsanctioned SaaS applications, and total bandwidth by SaaS sanctioned and unsanctioned applications. See Report types.
- Added support for sending reports as email attachments to selected recipients when the report is generated on demand and on schedule. This is configured by creating email groups using the *Manage email groups* button in *Analytics* > *Scheduled Reports* and by selecting email groups within the *Customize report* slide-in for a scheduled report. See Scheduling a report.
- Added user experience improvements to the *Network* > *Asset Map* for larger topologies including grouping multiple asset types and single asset types for global, regional, and local views, and hiding endpoints by default. Also, FortiAP edge devices are now shown by default on the asset map. See Network.
- Added datacenter support for Pune, India as a Fortinet Cloud Location. See Global data centers.
- Added datacenter support for Sydney, Australia as an endpoint management location. See Global data centers.

What's new for 23.4.49 (23.4.b)

- Added support for FortiFlex licensing in FortiSASE. FortiSASE entitlements created in the FortiFlex portal must be active for at least 90 days. See FortiFlex licensing.
- Added FortiSASE REST API support for configuring up to two IPsec overlays to two different WAN interfaces of a single SPA hub using BGP on loopback. See Appendix C - REST API.
- To provide integration with FortiGuard SOC-as-a-Service (SOCaaS), added the ability to configure log forwarding from FortiSASE to a SOCaaS collector using *Log Forwarding to SOCaaS* in *Analytics* > *Settings*. This feature requires an Advanced remote users FortiSASE license or a Comprehensive remote users FortiSASE license. See Forwarding logs to SOCaaS.
- Access to Public Cloud Locations and features included with the Advanced remote users FortiSASE license are now supported with the Comprehensive remote users FortiSASE license. See Global data centers.
- FortiSASE security PoP instances now have a feature release environment to support FortiGate Secure Edge and FortiAP edge devices.
- For new instances, the following networks are now available for your network configuration:
  - 10.8.0.0/16
  - 10.16.0.0/16
  - 100.64.0.0/10 (except 100.65.0.0/16)
  - 172.16.0.0/12
  - 192.168.0.0/16

  For existing instances, create a new FortiCare ticket to add support for these removed network restrictions. See Network restrictions removed.
- To provide administrators with an offline method for deregistering a FortiClient endpoint from FortiSASE Endpoint Management Service, added an option in *Configuration* > *Profiles* under the *Access* tab to enable allow disconnecting from FortiClient with password and to configure a password for this option. See Profiles.
- Added support in the FortiSASE Endpoint Management Service so that FortiClient endpoints prefer using DTLS, by default, when connecting to FortiSASE using VPN. If the endpoint attempts to use DTLS and fails due to network issues or otherwise, then it will fall back to TLS. If the endpoint does not support DTLS, then it will ignore the setting and prefer TLS. See Appendix D - VPN performance.
- Added datacenter support for the following Public Cloud Locations:
  - Amsterdam, Netherlands
  - Ashburn, Virginia, USA
  - Doha, Qatar
  - Hamina, Finland
  - Jakarta, Indonesia
  - Portland, Oregon, USA
  - Madrid, Spain
  - Melbourne, Australia
  - Milan, Italy
  - Santiago, Chile
  - Seoul, South Korea
  - Tel Aviv, Israel

  Access to these locations requires a Comprehensive remote users FortiSASE license. See Global data centers.

What's new for 23.4.31 (23.4.a)

- To allow administrators to adhere to privacy requirements, added support for configuring the FortiSASE log retention period from 2-30 days in *Analytics* > *Settings*. For existing instances, this feature remains disabled by default, which allows a default log retention period of 60 days until this setting is configured. New instances will have a default log retention period of 30 days. See Log retention policy.
- Added support for audit logging in the *Analytics* > *Events* > *Administrator Events* page of administrator login attempts and events, administrator FortiSASE portal configuration changes, and any changes made using the API or by an MSSP account. See Administrator Events.
- Added support for improved historical report data and formatting in *Analytics* > *Scheduled Reports* and *Analytics* > *Generated Reports*. See Scheduling a report, Manually running a report, and Report types.
- Added support for edge device connectivity using FortiAP, also known as FortiAP micro-branch. FortiAP micro-branch is a controlled General Availability feature with these requirements:
  - A separate FortiSASE subscription license per FortiAP. See the FortiSASE Ordering Guide.
  - FortiAP 231F and 431F devices running FortiAP firmware 7.2.4 and above.
  - The FortiSASE security PoPs running a feature release environment. If you require this support for your FortiSASE instance, contact FortiCare Support.

  See FortiAP.

Special notices

Removable media access

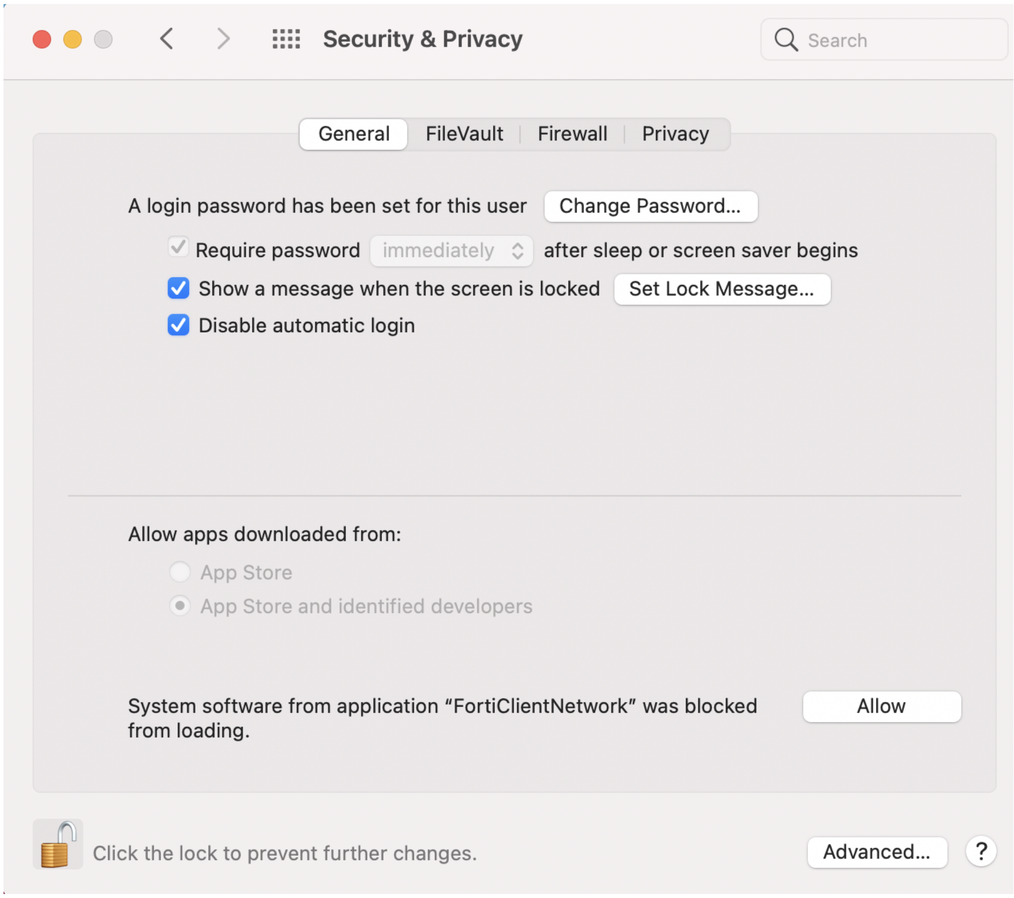
The *Profile* > *Removable Media Access Control* option only works if you enable Malware Protection, an optional feature, when installing FortiClient on the endpoint.

Activating the FortiClientNetwork extension

After you connect FortiClient (macOS) to FortiSASE, attempts to connect to SSL VPN may fail unless you enable the FortiClientNetwork extension. The FortiSASE team ID is AH4XFXJ7DK.

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*.



A login password has been set for this user

☑ Require password immediately after sleep or screen saver begins

☑ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

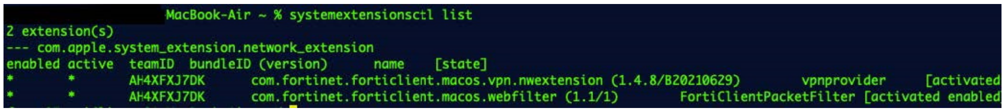
○ App Store

● App Store and identified developers

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

Click the lock to prevent further changes.

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



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

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.

Product integration and support

FortiSASE supports the following FortiClient versions:

- FortiClient (Windows) 7.0.11
- FortiClient (macOS) 7.0.11
- FortiClient (Linux) 7.0.11
- FortiClient (Android)
- FortiClient (iOS)

Use of earlier FortiClient versions with FortiSASE is not actively supported and may cause behavior differences.

Fortinet Support supports newer FortiClient versions even if they are not yet the recommended versions for FortiSASE.

FortiClient 7.0.11 is now the recommended version for FortiSASE for desktop users. FortiSASE has updated installers and download links to use FortiClient 7.0.11.

To provide improved performance and connectivity when connected to FortiSASE, for all existing managed endpoint users, each endpoint not running the currently available preconfigured installer of FortiClient 7.0.11 from the FortiSASE portal is prompted incrementally to upgrade to it. The user can perform this action immediately or schedule it to complete at a later time. See Managed endpoint client onboarding for details on the different FortiClient installer types. New tenants or those who requested that this feature be disabled on their instance will not automatically have this FortiClient managed endpoint enforcement feature.

Supported FortiClient features

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

Feature	Windows 7.0.11	macOS 7.0.11	Linux 7.0.11	Android	iOS
Managed Endpoints					
Diagnostic logs on-demand requests from FortiSASE	✓				
Digital experience monitoring agent support (requires Advanced or Comprehensive License)	✓	✓			

Feature	Windows 7.0.11	macOS 7.0.11	Linux 7.0.11	Android	iOS
FortiGuard Forensics Analysis support (requires Advanced or Comprehensive License)	✓				
Access					
Autoconnect to FortiSASE using Microsoft Entra ID credentials	✓				
Autoconnect to FortiSASE using SAML single sign on	✓	✓		✓	✓
Bypass FortiSASE using application-based split tunnel	✓				
Bypass FortiSASE using on-net endpoint detection via public IP address	✓	✓	✓		
Endpoint profile change notifications	✓	✓	✓		
Endpoint telemetry	✓	✓	✓	✓	✓
Endpoint VPN connectivity notifications	✓	✓	✓		
Endpoint VPN disconnection by disabling management connection from FortiSASE	✓	✓	✓		
Force always on VPN	✓	✓		✓	✓ The VPN toggle button is not disabled instantly. You must navigate away from the *VPN* page to disable the *VPN* button.
Split DNS	✓	✓	✓		
Show zero trust network access (ZTNA) tags on FortiClient	✓	✓	✓		✓ Does not support hiding tags.

Feature	Windows 7.0.11	macOS 7.0.11	Linux 7.0.11	Android	iOS
SSL VPN connection remains active after endpoint has been idle	✓	✓	✓		✓
SSL VPN support for DTLS*	✓	✓			
SSL VPN to FortiSASE	✓	✓	✓	✓	✓
Protection					
Antiransomware	✓				
Next generation antivirus (AV) – real-time AV and cloud malware protection	✓	✓	✓		
Removable media access control	✓	✓ FortiClient (macOS) does not support rules. It only supports allow and block actions.	✓ FortiClient (Linux) does not support rules. It only supports allow and block actions.		
Removable media access control – notify endpoint of blocks		✓	✓		
Vulnerabilities scanning	✓	✓	✓		
Sandbox					
Sandboxing - on-premise and FortiSASE Cloud Sandbox	✓	✓			
ZTNA					
ZTNA remote access	✓	✓	✓		
ZTNA tagging rules	✓	✓	✓	✓	✓

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

Common use cases

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

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

Use case	Description
SIA for FortiClient agent-based remote users on page 17	Secure access to the Internet using FortiClient agent.
SIA for FortiExtender site-based remote users on page 17	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 18	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 18	Secure access to the Internet using FortiAP device as FortiSASE edge device.
Log forwarding on page 18	Forward logs to an external server, such as FortiAnalyzer.
ZTNA on page 18	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases.
SPA using a FortiGate SD-WAN hub on page 19	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network.
SPA using a FortiSASE SPA hub on page 20	Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW).
SPA using a FortiSASE SPA hub with Fabric overlay orchestrator on page 20	Access to private company-hosted applications behind the FortiGate NGFW using Fabric Overlay Orchestrator .

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.

Use the following FortiClient versions:

- FortiClient (Windows) 7.0.11
- FortiClient (macOS) 7.0.11
- FortiClient (Linux) 7.0.11
- FortiClient (Android)
- FortiClient (iOS)

Use of earlier FortiClient versions with FortiSASE is not actively supported and may cause behavior differences.

SIA for FortiExtender site-based remote users

Currently, FortiSASE supports the FortiExtender 200F model for the LAN extension feature. The FortiExtender 200F should run 7.2.3. This feature requires a separate FortiSASE subscription license per FortiExtender.

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

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

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 21 for relevant issues resolved.

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

FortiGate SD-WAN as a secure edge is a controlled general availability (GA) feature that requires a separate FortiSASE subscription license per FortiGate. All FortiGate F- and G-series desktop platforms running FortiOS 7.4.2 and above can support FortiSASE Secure Edge connectivity.

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 16 FortiExtender and FortiGate devices combined that you can configure as FortiSASE edge devices.

SIA for FortiAP site-based remote users

FortiAP edge device support is a controlled GA feature that requires a separate FortiSASE subscription license per FortiAP. This feature supports FortiAP 231F and 431F devices running FortiAP firmware 7.2.4 and above.

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 32 FortiAP devices that you can configure as FortiSASE edge devices.

Log forwarding

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

ZTNA

If using the ZTNA feature, 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 secure private access (SPA) deployment using an existing FortiGate SD-WAN hub or SPA using a FortiGate NGFW converted to a standalone FortiSASE SPA hub. These SPA use cases are based on IPsec VPN overlays and BGP.

SPA Service Connection license

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

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

See the SASE and Zero Trust Ordering Guide.

SPA FortiCloud account prerequisites

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

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

For details on registering products, see Registering assets.

SPA using a FortiGate SD-WAN hub

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection license and SPA FortiCloud account prerequisites on page 19.

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
FortiManager	• 7.2.0 or later, which includes support for SD-WAN overlay templates • 7.0.3 or later, which includes BGP and IPsec VPN recommended templates for SD-WAN overlays
FortiClient	7.0.11

SPA using a FortiSASE SPA hub

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection license and SPA FortiCloud account prerequisites on page 19.

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
FortiManager	• 7.2.0 or later, which includes support for SD-WAN overlay templates • 7.0.3 or later, which includes BGP and IPsec VPN recommended templates for SD-WAN overlays
FortiClient	7.0.11

SPA using a FortiSASE SPA hub with Fabric overlay orchestrator

This use case requires a license per FortiGate device and requires each FortiGate device to be registered in the same FortiCloud account as FortiSASE. See SPA Service Connection license and SPA FortiCloud account prerequisites on page 19.

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
FortiClient	7.0.11

Resolved issues

The following issues have been fixed in version 24.1.56. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
943865	Filtering on FortiView Policies is inconsistent.
951989	Displaying installed applications for a newly connected endpoint takes about 50 minutes for some tenants.
955238	Reauthorizing a deauthorized FortiExtender does not work without rebooting the FortiGates.
955572	Microsoft Entra ID autoconnect configuration does not display all information on the GUI. Functionality works as expected.
957574	Installed applications for an endpoint on *Managed Endpoints* does not display all results.
957742	Deletion of DNS rule with domain longer than 36 characters displays an error.
969882	Secure private access public API: region cost does not show all the PoPs in the API response.
970055	*Unable to fetch FortiView Data* displays on *Status* dashboard when logged in as read-only user.
975160	Administrator Event logs do not show on FortiSASE in real time.
981356	DTLS may fall back to TLS when using SAML SSO on FortiClient (Windows).
999792	*Management Connection* filter in *Managed Endpoints* table may not return accurate results.
999955	Hosts and feeds cannot have the same name.
1003287	When a FortiExtender is authorized, the IPsec VPN tunnel interface does not receive an IP address causing traffic disruption for endpoints connected to the FortiExtender. Existing instances require a workaround. See SIA for FortiExtender site-based remote users on page 17.
1003695	Error displaying website content compressed with zstd such as Facebook, WhatsApp, or Instagram websites.
1021511	Cannot log in to tenants with NFR licenses.

Known issues

The following issues have been identified in version 24.1.56. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
638426	For secure web gateway (SWG) users, loading some websites using cookie-based authentication or websites that do not allow redirection has issues. **Workaround**: customize PAC file that SWG users use to exempt affected websites.
716833	FortiClient (macOS) does not support application-based split tunneling.
746224	Clicking *Deauthenticate* for a SWG user in *Session Monitor* does not deauthenticate the user.
749159	FortiSASE performs SWG authentication via HTTP. Therefore, single sign on (SSO) authentication is strongly recommended for SWG users.
775860	When installing FortiClient 7.0.8 on Windows, user may see a warning about FortiClient originating from an unknown publisher if Windows Defender is enabled.
837391	*Connected Users* and *Asset Map* display *0.0.0.0/Unknown IP* for VPN SSO users.
888092	Changes made to a modified proxy policy may not always take effect.
907570	FortiSASE currently does not support option to test SAML connectivity for SWG SSO.
914278	*Managed Endpoints* incorrectly displays warning for FortiClient version mismatch for iOS and Android devices.
964123	Custom endpoint profiles cannot use LDAP server configured before FortiSASE instance upgrade to 23.4. **Workaround**: edit existing LDAP server configuration from first page and reenter credentials. See Profiles for details.
998070	Only a root user can access Forensics services in a managed security service provider setup.
1015248	Option to add and modify threat feeds may not always display on GUI.
1019049	Message prompt does not display when requesting FortiClient debug logs from the *Endpoint Details* window.

Limitations

FortiClient desktop (Windows, macOS, Linux)

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- For an endpoint to be able to connect to FortiSASE via an SSL VPN tunnel, the FortiSASE environment must have at least one SSL VPN allow policy configured. See Adding policies to perform granular firewall actions and inspection.

FortiClient Android

On certain Android devices, when the CA certificate is downloaded from FortiSASE and manually installed on an Android device, untrusted certificate warnings for this certificate are seen constantly. This behavior is the result of Android system limitations on certain devices.

FortiClient Cloud

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

Authentication

- Other methods of user authentication will not work once SAML SSO is enabled.
- Not all options for LDAP server configuration are available on FortiSASE.
- Deauthenticating a Secure Web Gateway SSO user does not direct user to reauthenticate on device without clearing browser cache first.

FortiSandbox

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

Release Notes

FortiSASE 24.1.56