Release Notes

FortiSASE-Sovereign 26.2.a

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 30, 2026
FortiSASE-Sovereign 26.2.a Release Notes

TABLE OF CONTENTS

Change log

Date	Change Description
2026-03-13	Initial release.
2026-04-30	Updated: • What's new • Other considerations • Product integration and support • Resolved issues • Known issues • Limitations

Introduction

This document describes the new features, functional enhancements, special notices, and known issues included in the FortiSASE-Sovereign 26.2.a. It is strongly recommended to review all sections of these release notes prior to deployment or upgrade to fully understand feature changes, behavioral modifications, and service impact.

For the latest documentation and product information, visit:

https://docs.fortinet.com/product/fortisase-sovereign

What's new

What's new for 26.2.a

- MSSP tenant VDOM deletion
  - MSSP administrators can now delete tenant VDOMs directly from the MSSP portal. When a VDOM is deleted, the system automatically recreates a clean VDOM on the Security PoP FortiGate, making it available for assignment to other tenants.
- IPsec VPN Support for Windows Endpoints in Shared and Dedicated NAT Topologies
  - FortiSASE-Sovereign now supports IPsec VPN deployments using Shared NAT and Dedicated NAT topologies, including environments that require non-default IKE ports. This capability is supported for Windows endpoints running FortiClient 7.4.6 or later.
- Improved GSLB failover in dedicated mode
  - Fixed a critical issue affecting users upgrading from GA 1.0, which could cause GSLB failover to fail.
- Dedicated Instance IAM Administrator Support
  - FortiSASE-Sovereign now supports creation of a Dedicated_Admin permission type for Dedicated Instance deployments.
  - Administrators can now create Dedicated_Admin users.
  - The Dedicated_Admin type permission includes full tenant portal permissions and dedicated portal permissions.

What's new for 26.1.a

- FortiSASE-Sovereign 2.0 introduces two tenancy models to support different deployment scenarios:
  - Dedicated Instance
  - Multi-Tenant Instance (MSSP model)

  These models provide flexible management and operational structures based on customer requirements.
- The MSSP Admin Portal enables centralized management of multiple tenant environments from a single interface.

  Key capabilities include:

    - Tenant lifecycle management (create, edit, delete, direct portal access)
    - Portal component and system health monitoring
    - IAM user management for both MSSP and tenant portals
    - License status review across all managed tenants
    - Controller and Security PoP resource management
    - Scheduled FortiOS upgrades for PoP FortiGate devices

  The portal is functionally organized into the following modules:
    - Monitor – View portal component status and deployment regions
    - Tenant – Manage tenant accounts and access tenant portals
    - IAM – Manage local users and configure IdP-based authentication
    - License – Review entitlement status
    - Asset – Manage controllers and monitor Security PoP resource usage
    - Maintenance – Schedule FortiOS upgrades for PoP FortiGates
- The Dedicated Instance model provides management capabilities scoped to a single tenant environment.

  Available features include:
    - IAM user creation and permission profile assignment
    - License status visibility
    - Scheduled FortiOS upgrades for PoP FortiGate devices
    - This model is optimized for customers requiring isolated management without multi-tenant administration.
- MSSP License Status Management Enhancements
    - Improved license visibility is now available for MSSP deployments.
    - Dedicated environments include a centralized License page displaying entitlement details for Sovereign SASE, FortiAnalyzer (FAZ), and FortiGate (FGT).
    - In multi-tenant deployments, license information is presented within each tenant's License Details tab.
- MSSP License Resource Recycling and Enforcement
    - Automated license monitoring has been introduced to enforce entitlement compliance and reclaim resources. **A daily watchdog task validates license status and may trigger controller group, account, or FortiGate (FGT) deletions when licenses expire or are decommissioned.**
    - EMS and Portal licenses generate reminders 30 days prior to expiration. Post-expiration grace periods and automated deletion policies are enforced based on license type.
    - Tenant eligibility is validated daily against EMS contracts. Expired tenants or tenants without sufficient seats are un-onboarded, and associated EMS, FMG, FAZ, and FGT resources are automatically released.
- MSSP System Maintenance – FortiOS Upgrade Service
    - A new system maintenance upgrade service has been introduced to support controlled PoP FortiOS (FOS) firmware upgrades across all tenants and devices.
    - Upgrades are initiated by the FortiSASE-Sovereign DevOps team and executed through FortiManager (FMG) using scheduled upgrade templates. Administrators can adjust the maintenance window and notification frequency prior to execution.
    - During the upgrade window, the tenant portal is temporarily unavailable and is automatically restored upon completion. No tenant action is required.
- Multi-Region Controller Onboarding

    - The controller can now onboard multiple FortiGate devices across different PoP regions.
    - This enhancement enables distributed deployments with improved geographic flexibility, allowing organizations to scale infrastructure across regions while maintaining centralized orchestration.
- Multi-Tenant Onboarding with Multi-VDOM Support
    - Tenant onboarding now supports multiple FortiGate VDOMs per tenant, with one VDOM selected from each FortiGate.
    - This allows each tenant to operate with segmented virtual domains, enabling improved resource isolation, scalability, and flexible deployment architectures within shared infrastructure environments.
- Enhanced MSSP Tenant Capacity Management
    - MSSP administrators can now define a maximum user allocation per tenant.
    - The total number of users assigned across tenants under a single controller must not exceed the EMS license seat capacity associated with that controller. This provides improved resource governance and clearer license utilization control.
- Expanded VDOM Support in Tenant Portal
    - VDOM-based architecture is now further integrated across Tenant Portal workflows, including:
        - Endpoint Management Profiles
        - ZTNA tagging and application definitions
        - DNS configuration
        - IPsec VPN configuration
    - This enables more flexible segmentation and advanced policy control in multi-tenant environments.
- Dedicated Instance Tenant Onboarding
    - Support for Dedicated Instance onboarding is now available.
    - Customers can deploy and manage a fully isolated tenant environment with dedicated resources, providing enhanced control, operational independence, and simplified governance.
- Authenticated EMS Invitation Code
    - Security has been enhanced for endpoint onboarding.
    - Users are now required to authenticate before establishing a connection between the endpoint and FortiClient EMS when using an invitation code.
    - Supported authentication methods include:
        - Active Directory (AD)
        - Microsoft Entra ID (Azure AD)
    - This change strengthens identity verification and reduces the risk of unauthorized endpoint registration.
    - Limitation: FortiClient for Android and iOS is not supported in this release.
- Simplified Pre-Logon Tunnel Support
    - Pre-logon tunnels have been simplified to improve deployment consistency and security.
    - Endpoints now establish certificate-based tunnels to the nearest FortiSASE-Sovereign Security PoP. The simplified model supports shared destination policies and requires an SPA hub with connectivity to an Active Directory server.
    - Supported Platforms
        - Windows 10
        - macOS
- External Threat Feed Support

    - Support for external threat feeds has been introduced, allowing dynamic import of IP address, domain name, and URL lists from remote servers.
    - External feeds can be applied as follows:
        - IP Address feeds in Firewall and SWG policies (source and destination)
        - Domain feeds as custom FortiGuard categories in DNS Filter
        - URL feeds as custom FortiGuard categories in Web Filter
    - Administrators can configure refresh intervals and enable secure HTTPS retrieval with authentication. Each FortiSASE tenant supports up to 20 external feeds.
- IAM Enhancements
    - Enhanced IAM capabilities are now available for managing authenticated access to MSSP and Tenant portals.
    - Administrators can create Local Users (username and password) and integrate external Identity Providers (IdP) using SAML-based SSO, including support for Microsoft Entra ID and FortiAuthenticator.
    - User roles can be assigned as MSSP type (access to MSSP and Tenant portals) or Tenant type (single-tenant access). Granular Permission Profiles are also supported to define read, write, or no-access privileges.
- Firewall Inspection Mode Configuration
    - Support for configuring firewall inspection mode prior to tenant onboarding has been introduced.
    - The system supports two inspection modes that define how firewall policies process traffic:
        - Flow-based – Only flow-mode policies are permitted.

          Note: Custom DNS rules are not supported in this mode.
        - Proxy-based – Only proxy-mode policies are permitted.
- SSL Inspection Enhancement
    - Support for the No Inspection mode has been added to SSL Inspection, allowing traffic to bypass SSL/TLS inspection when required.
- Multi-Profile Endpoint Configuration
    - Endpoints can now be assigned different management profiles.
        - For AD users, profiles can be automatically applied after endpoint login using AD credentials.
        - Non-AD endpoints can be manually assigned to profiles by administrators after connection.
    - This improves endpoint policy flexibility and user-based configuration control.
- Transparent DNS-Based Split Tunnel
    - DNS split tunneling is now implemented using a transparent DNS database within the DNS Filter security profile.
    - Only users matched by proxy-based firewall policies with DNS filtering enabled can use DNS split tunnel. Flow-based users are not supported.
    - Changes to DNS rules or system DNS settings may reset existing IPsec VPN sessions.
- Comprehensive On-Net Rule Sets
    - On-Net rule definitions now support additional matching criteria, including:
        - Public IP
        - DNS
        - DHCP
        - Subnet
        - Ping

    - This allows more granular and flexible detection of on-network conditions.
- Source NAT (SNAT) Control for SPA Policies
    - Source NAT (SNAT) for Secure Private Access (SPA) firewall policies can now be enabled or disabled.
    - By default, NAT remains enabled. However, MSSP 2.0 introduces the option to disable SNAT when preserving the original client source IP address is required.
    - This enhancement allows:
        - Greater transparency for traffic visibility
        - Improved compatibility with upstream systems that rely on original client IP
        - More flexible SPA deployment models
    - SNAT settings can be configured directly in the FortiSASE-Sovereign GUI.
- IP Address Management (IPAM)
    - A new built-in IP Address Management (IPAM) capability is now available in FortiSASE-Sovereign.
    - IPAM automatically manages IP pools and assigns non-overlapping subnets to:
        - FortiClient dial-up IPsec tunnels
        - Pre-logon IPsec tunnels
        - Thin-edge devices
    - This reduces manual IP planning and eliminates subnet conflicts across deployments.
    - Key capabilities include:
        - Automatic subnet allocation
        - Subnet release and reuse
        - Default pool management
    - IPAM operates natively within the FortiSASE-Sovereign platform and is fully integrated into system workflows.
- SSL VPN Removed
    - To enhance overall Secure Internet Access (SIA) security posture, SSL VPN is no longer supported.
    - Existing deployments must migrate to IPsec VPN prior to upgrading to the MSSP version.

What's new for 25.3.a

- Multiple Orchestration Regions Support
    - To improve performance, support data residency, and provide a better user experience for global customers, FortiSASE-Sovereign now supports Multiple Orchestration Regions. This enhancement allows users to be automatically redirected to the regional FortiSASE-Sovereign portal based on their account's region, reducing latency and improving regulatory compliance (e.g., GDPR).
    - During initial login, users without an assigned region will be prompted to select one, which will be remembered for future access.
    - Key benefits include:
        - Seamless regional onboarding and login experience
        - Up to 50% improvement in latency through region-aware routing
        - Better support for data sovereignty and compliance

    - Simplified DevOps operations with configuration-based region setup
    - Clear regional identification through portal subdomains
- Flow-based security policy and profile group support
    - Flow-Based Inspection Mode is now supported in FortiSASE-Sovereign firewall policies, enhancing flexibility and improving performance.
    - Administrators can choose between Flow-Based (now the default) and Proxy-Based inspection modes when creating firewall policies.
    - Each inspection mode requires a compatible security profile group:
        - Default (Flow-Based)
        - Default-Proxy (Proxy-Based)
    - The UI clearly distinguishes inspection modes and dynamically filters unsupported features based on the selected mode.
    - Proxy-Based mode continues to support advanced features such as Inline-CASB Headers, while Flow-Based mode is optimized for higher performance and lower resource consumption.
    - All supported security profiles can be used in either mode, but feature availability may differ (e.g., some Web Filter options are only available in Proxy mode).
    - Upgrade behavior:
        - Existing default profile group renamed to Default-Proxy
        - A new Flow-Based profile group named Default is created
        - Custom user-defined policies/profile groups remain unchanged (in Proxy mode)
        - SIA and SPA default policies may migrate to Flow-Based mode unless modified

What's new for 25.2.a

- **Comprehensive SASE solution with seamless deployment** — FortiSASE-Sovereign provides a turnkey solution that includes all essential components for a fully integrated SASE architecture, such as Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), and Cloud Access Security Broker (CASB).
- **Full autonomy and operational control** — Organizations retain complete control over where and how their SASE services are deployed, ensuring customized security and networking policies tailored to specific business needs and regulatory requirements.
- **Data sovereignty and compliance** — FortiSASE-Sovereign ensures that sensitive data remains within the designated jurisdiction, allowing organizations to comply with data localization regulations while maintaining full ownership and privacy of security logs and records.
- **Innovative architecture** — The solution is designed with a modern architecture that separates core functionalities from data control, optimizing cost efficiency, deployment speed, and operational flexibility.
- **Simplified licensing and scalability** — FortiSASE-Sovereign offers a straightforward purchasing model, allowing organizations to easily scale based on user capacity. This streamlined approach ensures cost-effective adoption and deployment.

Special notices

When onboarding FortiSASE-Sovereign 26.2.a, pay special attention to the notes regarding the use of the following system components and/or features:

FortiGate/FortiOS

- **Product registration and activation** — Before onboarding your FortiGates, you must register and activate the devices one or two days ahead of time.
- **Check for log hard disk** — Before onboarding, be sure to check the log disk status using the following CLI command:

  ```
  get system status
  Log hard disk: Available
  ```

  If the log hard disk is not available, format the hard disk using the following CLI command:

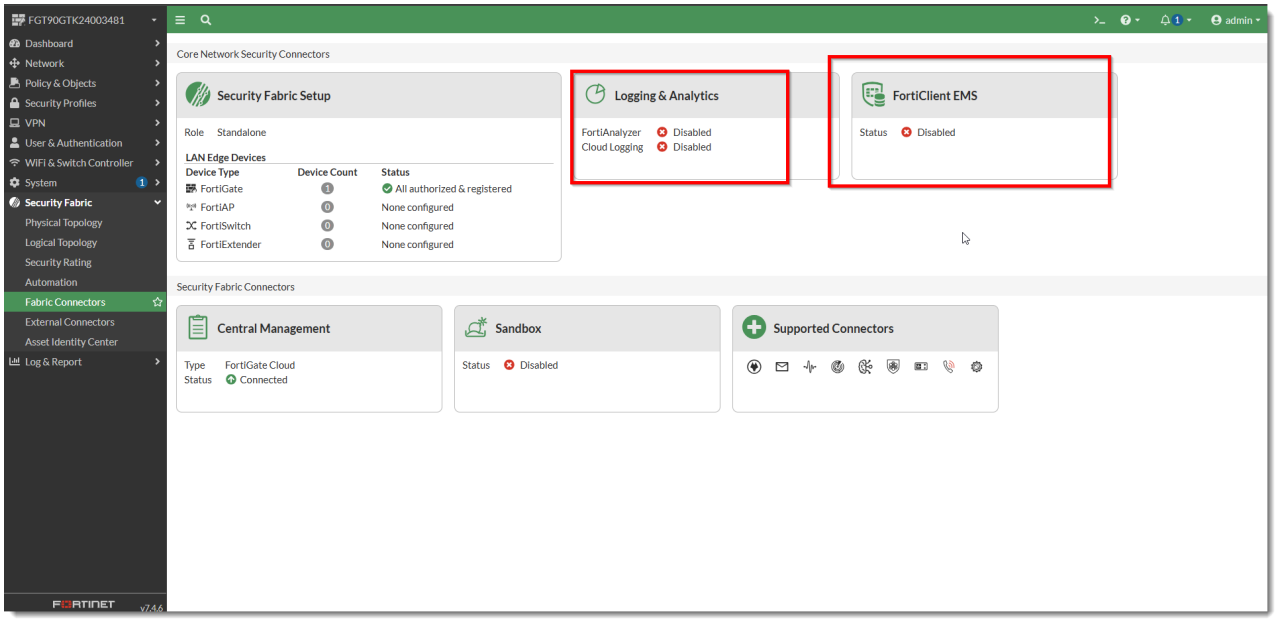
  ```
  execute formatlogdisk
  ```
- **Two-Ports topology** — Before onboarding, ensure that the default route on the PoP FortiGate is configured to use the egress port. If static routes are used, try to assign a lower priority value to the default route via the egress port because a lower value denotes a higher routing priority.
- **Single-arm topology** — Before onboarding, ensure that the default route of the PoP FortiGate is through the egress port.
- **Activate FortiGate via FortiGate Cloud** — You must activate your FortiGate using FortiGate Cloud, and make sure that *both Logging & Analytics and FortiClient EMS are disabled*, as illustrated in the following code sample and screenshot:

  Register and activate FortiGate devices at least 48 hours before onboarding to allow licensing and cloud services to fully synchronize.

  ```
  config log fortianalyzer setting
  end
  config endpoint-control fctems
      edit 1
      next
  ```

```
    edit 2
    next
    edit 3
    next
    edit 4
    next
    edit 5
    next
    edit 6
    next
    edit 7
    next
end
```



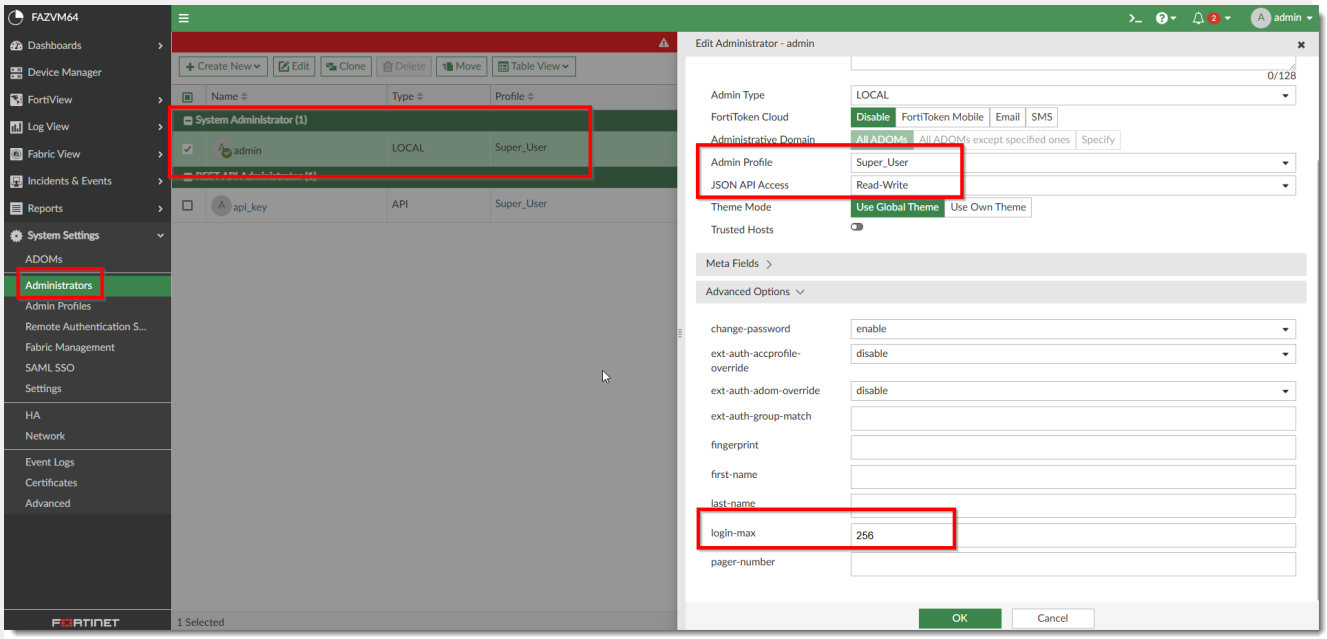
After onboarding, you (the administrator) can access the FortiGate through its Port 5443 using the HTTPS protocol.

FortiAnalyzer

You must enable the system admin user to have JSON-RPC read-write permissions and set login-max to 256, as illustrated in the following code sample and screenshot:

```
config system admin user
    edit "admin"
        set login-max 256
        set password ENC SH24n/hcS8Hnq5ancSHxkVat7tFyCgw4MBd/tBXgL/oYFUlREMmq6O6qA+gzxs=
```

```
        set profileid "Super_User"
            config meta-data
                edit "Contact Email"
                next
                edit "Contact Phone"
                next
            end
        set rpc-permit read-write
    next
end
```



Download FortiClient for onboarding users

If the FortiClient installer is unavailable or fails during user onboarding, click the *Retry* button to regenerate the installer and repeat the process until the download is successful.

Authentication

- IPSec VPN does not support LDAP authentication.
- Authentication Method Priority Order

  - The authentication method is evaluated in the following priority order:
    - Automatic Sign-On (OIDC)
    - SAML Single Sign-On (SSO)
    - Other authentication methods (LDAP, RADIUS, and Local User)
  - The behavior is as follows:
    - When Automatic Sign-On (OIDC) is enabled, it takes highest priority. SAML SSO and all other authentication methods will not be triggered.
    - When Automatic Sign-On (OIDC) is disabled and SAML SSO is enabled, SAML SSO takes priority over all remaining authentication methods.
    - Only when both Automatic Sign-On (OIDC) and SAML SSO are disabled, LDAP, RADIUS, and Local User authentication methods will be evaluated.
- Note: Only one authentication method is processed based on the priority order. Lower-priority authentication methods are not evaluated if a higher-priority method is enabled.

Secure Private Access (SPA)

While configuring SPA, ensure that the same ADVPN route tag number is configured across all service connections for each BGP on the loopback peer on the SPA/SD-WAN portal.

Secure Web gateway (SWG)

- To ensure that SWG access functions correctly, Deep Packet Inspection (DPI) must be enabled in the SWG proxy security profile groups for both:
  - Internet Access
  - Private Access
- If Deep Packet Inspection is not enabled for both profile groups, SWG access may not operate as expected.
- Note: This requirement applies to all deployments using SWG proxy-based security profiles for Internet and Private Access traffic.

Other considerations

- Custom DNS rules apply only to proxy-based firewall policies.
- The edge-dns-exempt-Proxy profile cannot be cloned. This profile is reserved for edge device usage only.
- Firewall policy type and security profile type must match. For example, proxy-based policies require proxy-based profiles.
- Profile cloning is limited to profiles of the same type. Profiles cannot be cloned across different profile types.

- The Dedicated_Admin type is supported only in Dedicated mode.

Product integration and support

FortiSASE-Sovereign supports the following FortiClient versions:

- FortiClient (Windows): 7.4.6 2001
- FortiClient (macOS): 7.4.6 1926
- FortiClient (Linux): 7.4.6 1867

Note: Android and iOS platforms are not supported at this time. Support for these platforms will be introduced in a future release.

If the PoP deployment uses the NAT topology, please contact Technical Support to obtain the required special build of FortiClient.

FortiSASE-Sovereign requires a special build of FortiOS to operate:

- FortiGate: 7.4.11 6843
- FortiAnalyzer: 7.4.10 GA or later

Common use cases

FortiSASE-Sovereign works in tandem with some other Fortinet products to meet your network connectivity, security, and compliance needs. The following table highlights some common use cases of FortiSASE-Sovereign with other compatible Fortinet products:

Use case	Description
Secure Internet Access (SIA) for FortiClient agent-based remote users	Secure access to the internet using FortiClient agent.
SIA for FortiExtender site-based remote users	Secure access to the internet using ThinEdge FortiExtender device as FortiSASE-Sovereign LAN extension.
SIA for FortiAP site-based remote users	Secure access to the internet using FortiAP device as FortiSASE-Sovereign edge device.
Log forwarding	Forward logs to an external server, such as FortiAnalyzer.
ZTNA	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	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network.
SPA using a FortiSASE-Sovereign SPA hub	Access to private company-hosted applications behind the FortiGate next generation firewall (NGFW).

SIA for FortiExtender site-based remote users

In this scenario, FortiSASE-Sovereign uses FortiExtender as its LAN extension. It requires FortiExtender Model 200F running on FortiExtender firmware 7.6.0 or later.

- Random port configuration is not supported for FortiExtender and FortiAP.
- To take full advantage of FortiSASE-Sovereign, the FortiGate device used as a Thin Edge must also use the same NPI version as the one used on the PoP FortiGate.

SIA for FortiAP site-based remote users

This use case requires FortiAP firmware 7.6.0 or later running on the following hardware devices:

- FortiAP 231F
- FortiAP 431F

SPA

FortiSASE-Sovereign supports SPA deployment in the following scenarios:

- Using an existing FortiGate SD-WAN hub
- Using a FortiGate NGFW converted into a standalone FortiSASE-Sovereign SPA hub

- Both of these SPA deployment models utilize IPsec VPN overlays and BGP for secure connectivity.

SPA using a FortiGate SD-WAN hub

This use case needs the regular FortiGate, FortiCare, and FortiGuard licenses. No special license is required.

SPA using a FortiSASE-Sovereign SPA hub

This use case needs the regular FortiGate, FortiCare, and FortiGuard licenses. No special license is required.

Resolved issues

The following issues have been resolved in version 26.2.a Feature. For questions regarding a specific bug, please contact Customer Service & Support.

Bug ID	Description
1077750	LDAP Server creating/editing page missing Access Type with its tooltip description.
1236111	When IPsec VPN gateway is behind NAT device with vip mapping, No downstream traffic after tunnel is up.
1252178	Multi-Tenancy failed to create FortiAnalyzer ADOM during tenant onboarding when limit is reached.
1256494	Failed to reach the AD server behind the SPA with BGP loopback.
1266173	GSLB may direct traffic to an offline PoP FGT.
1266345	Multiple status errors in health status screen.
1281352	The function of creating ZTNA tag in security policy is incomplete.

Known issues

This release of FortiSASE-Sovereign 26.2.a has the following known issues.

Bug ID	Description
1138441	FortiGate operating in Thin-Edge mode does not support arbitrary modification of the control port.
1170662	Support IKEv2 IPsec auth with PSK + EAP enabled.
1221681	Multi-Tenancy MSSP Controller onboarding failed after reset FortiGate using factoryreset2.
1234056	[Tracking 1234051] Tracking auto-connect save username/password issue.
1236725	Using the invitation code for Microsoft Entra ID domain fails to connect to EMS.
1238114	Throws the "Protocol timeout reached" error when trying to connect to IPSec VPN.
1242845	Multi-Tenancy Tenant onboarding with adding 901G PoP FortiGate failed due to FortiManager auto retrieve action during onboarding.
1250122	Multi-Tenancy unable to deploy multiple tenant concurrently, must wait for the previous tenant deployment to complete then start the current one.
1251362	Multi-Tenancy MSSP Controller onboarding FortiManager got some Install Device task failed.
1279072	Expired tenant not able to enter from MSSP Portal but able to access when user switch tenant in tenant portal.
1282548	VDOM Deletion: When delete more than 3 VDOM in a batch, deletion will fail due to VDOM tag removal failure.
1282893	Tenant settings display is truncated in laptop screen if resolution is not high enough.
1283625	In Analytics-Logs, filter log with Admin-Ro permission will return 500 error in API response.

Limitations

EMS license registration and upgrade guidelines

You must register only one EMS user license and perform all upgrades on this same license. Registering multiple licenses may cause the following issues:

- The Portal will prioritize the oldest EMS license, meaning all add-on users must be registered under this license.
- If multiple EMS licenses are registered, they will be activated sequentially based on their activation date.
- If multiple EMS licenses are registered and the oldest license expires without renewal, the next oldest license will be used instead. In that case, you must re-register add-on users under the newly activated license.

To avoid potential issues, we strongly recommend using and maintaining a single EMS user license and upgrade it when needed.

DNS Split Tunnel

DNS split tunneling is supported only for users operating under proxy-based inspection mode. Flow-based users are not supported.

Changes to DNS rules may cause existing IPsec VPN sessions to reset.

Active Directory Integration

To use Active Directory users in endpoint management profiles, the AD domain must first be configured in the FortiSASE-Sovereign portal.

Only users from configured AD domains can be assigned to endpoint management profiles.

IAM User Management

- Multiple local IAM users cannot be registered using the same email address.
- For local IAM accounts, password changes are supported only through email-based password reset.

External Feeds

Each tenant supports a maximum of 20 external feeds.

Unsupported Configurations for VDOM Deletion

- VDOM deletion is currently not supported for tenants with the following configurations. Before deleting VDOMs, remove any unsupported configurations:
  - Thin-edge FortiExtender.
  - Thin-edge FortiGate.
  - Thin-edge FortiAP.
  - Custom Web Filter categories with Threat Level enabled.

www.fortinet.com