Administration Guide

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 Administration Guide

TABLE OF CONTENTS

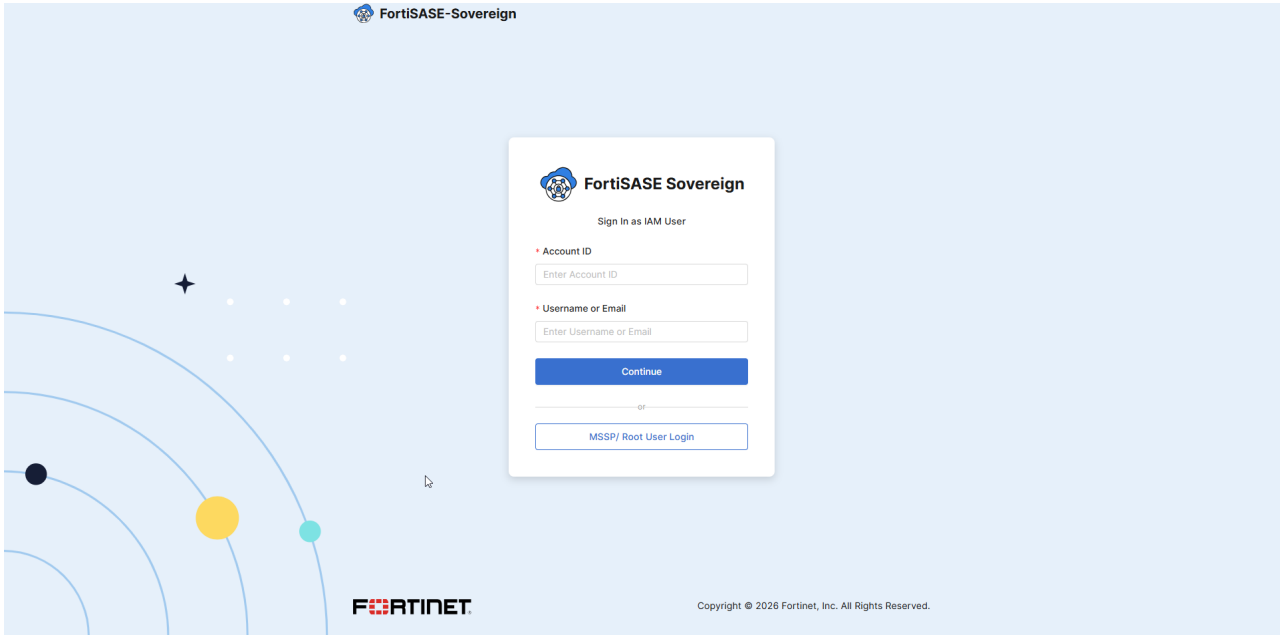
Change Log

Date	Change Description
2026-04-30	Initial release.

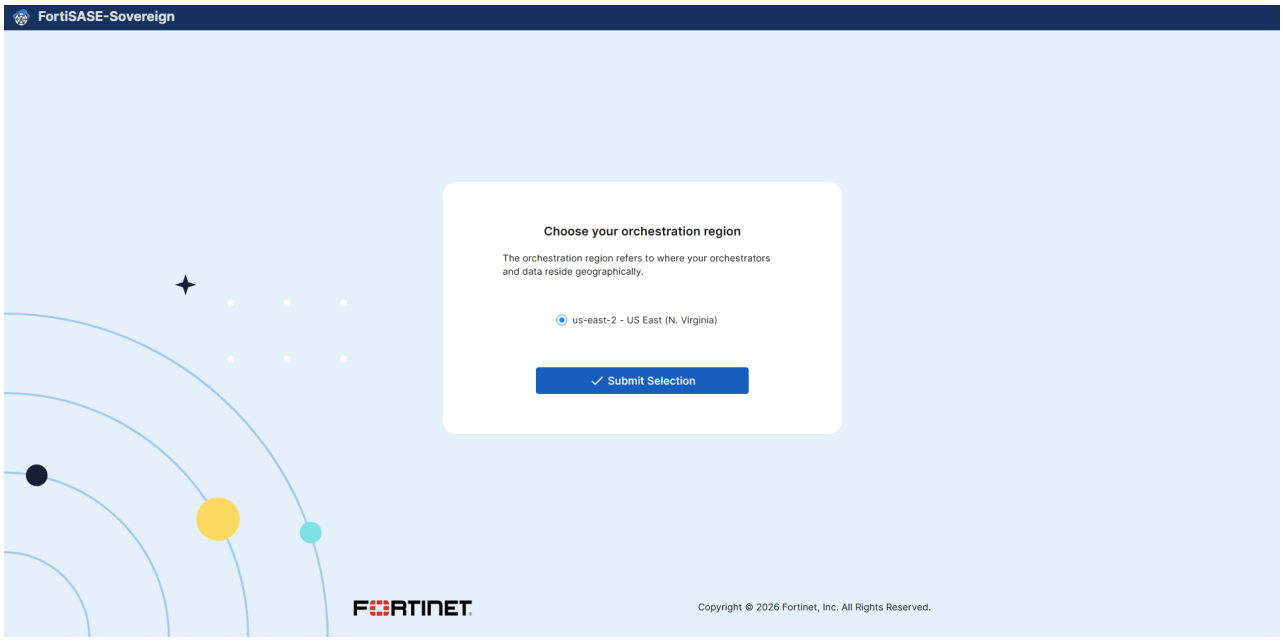
Multi-Tenancy Onboarding

Login Landing Page

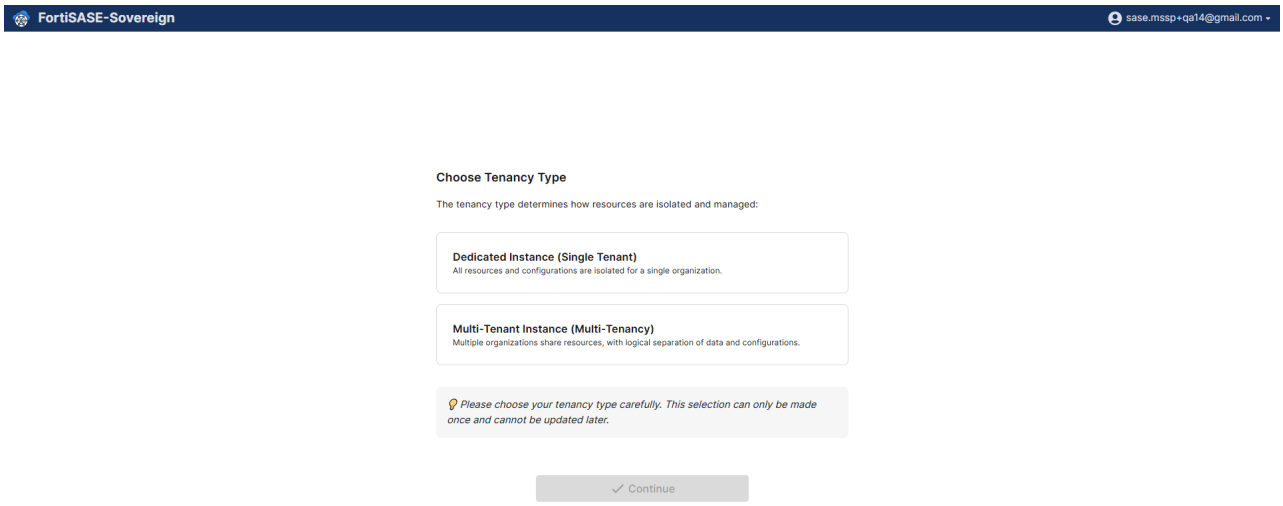
1. Log in using your MSSP (root) administrator account. This account provides full access to manage all tenants and system configurations.



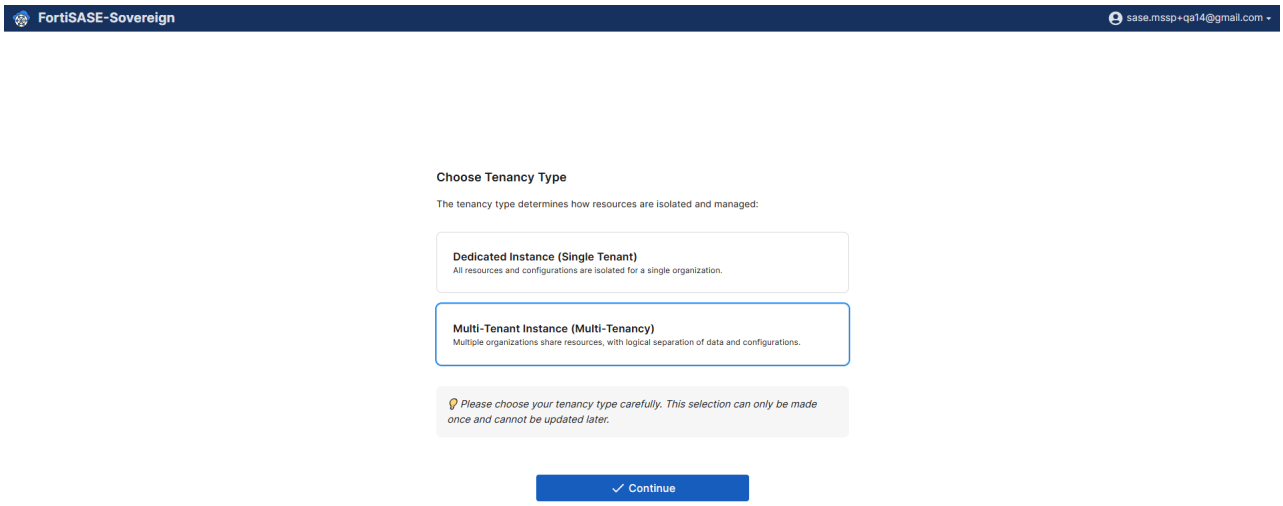
2. Select the appropriate orchestration region based on your deployment location and compliance requirements, then click Submit. The selected region determines where the management plane infrastructure will be provisioned and governs data residency boundaries for all tenants under this MSSP account.



3. Select the tenancy model that fits your deployment: choose Dedicated Instance (Single Tenant) for an isolated, single-customer environment, or Multi-Tenant Instance (Multi-Tenancy) to enable a shared infrastructure model that supports multiple managed tenants under a single MSSP controller. This choice defines how your environment is structured.
   - Note: This tenancy selection is a one-time, permanent configuration that cannot be modified after the initial setup is complete. Ensure the correct deployment model is selected before proceeding.

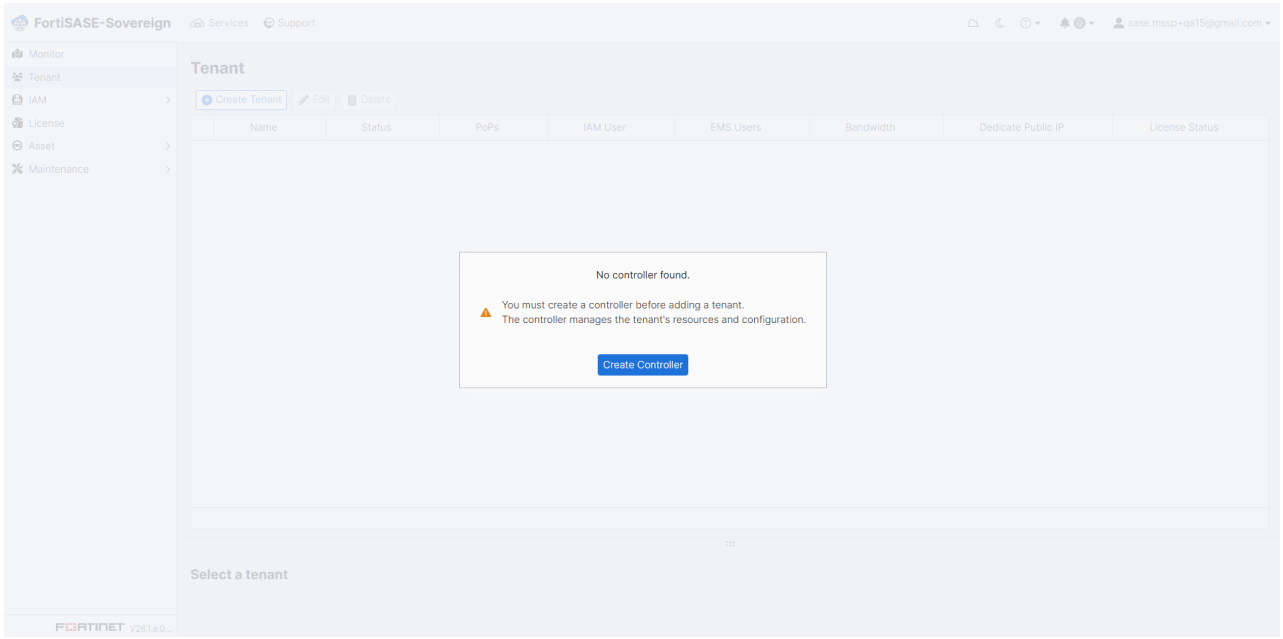


4. Select Multi-Tenant Instance (Multi-Tenancy) as the deployment model to enable the full MSSP multi-tenancy feature set, and then click Continue to proceed to the controller configuration phase. This option activates the shared infrastructure framework required for managing multiple independent tenant environments.

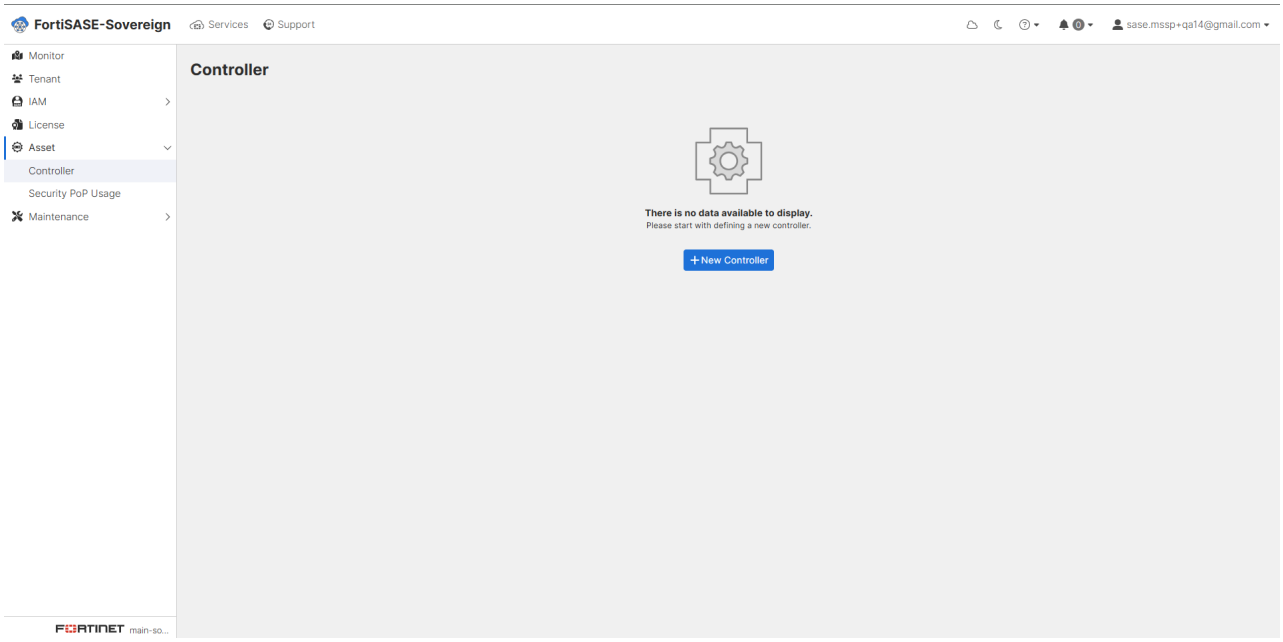


Controller Onboarding

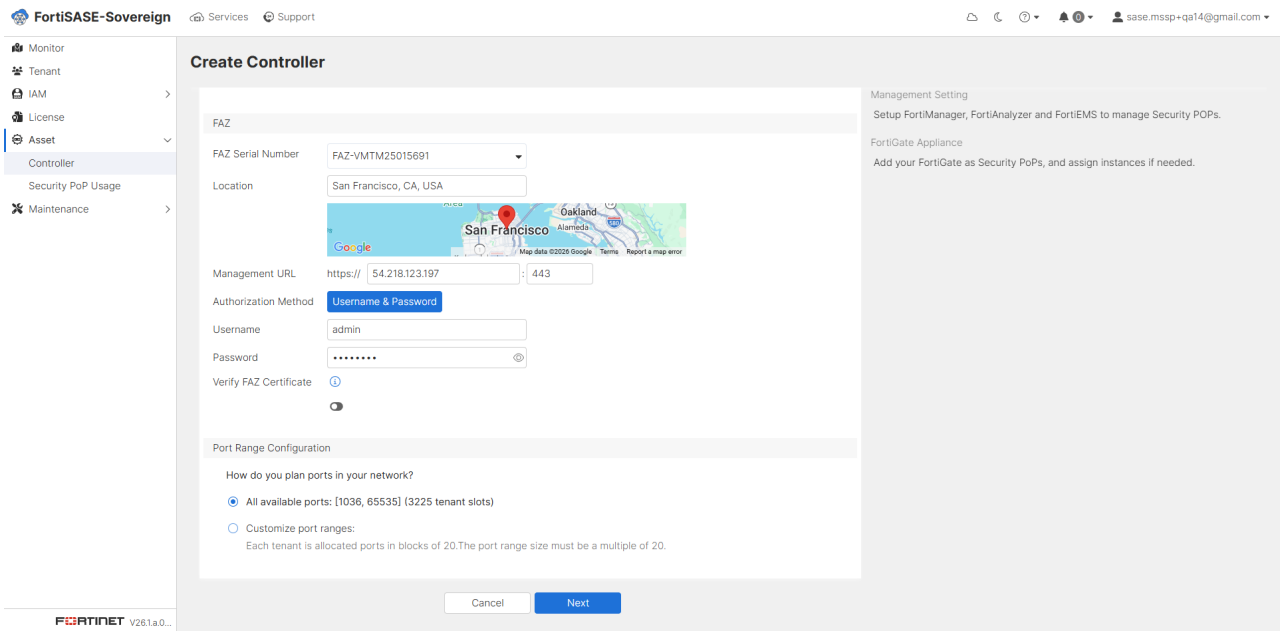
1. If no controller is configured, the system will prompt you and display a “No Controller Found” notification dialog. Click Create Controller within this dialog to initiate the controller provisioning workflow. A controller is required before any tenant onboarding or security policy management can take place.



2. Go to Asset > Controller in the portal, then click +New Controller to begin registering a new controller instance. The Asset Controller serves as the central management node responsible for orchestrating security policies, tenant segmentation, and FortiGate integration across the Multi-Tenant Instance.

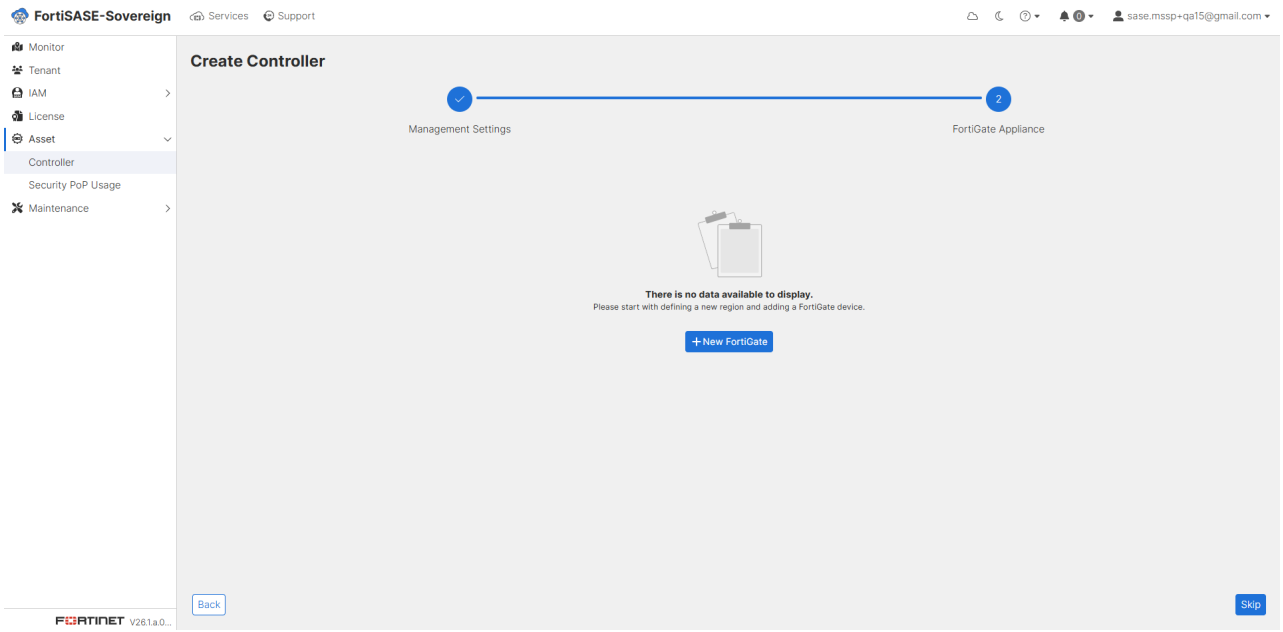


3. Enter the required controller details: enter a descriptive Controller Name, select the associated FortiClient EMS Serial Number from the available inventory, choose the target deployment Region, select the corresponding FortiAnalyzer Serial Number for log aggregation, and specify the physical or logical Location. Additionally, enter the Management URL along with valid administrator Username and Password credentials, and define the Port Range Configuration to govern VDOM allocation. Once all fields have been populated, click Next to proceed.

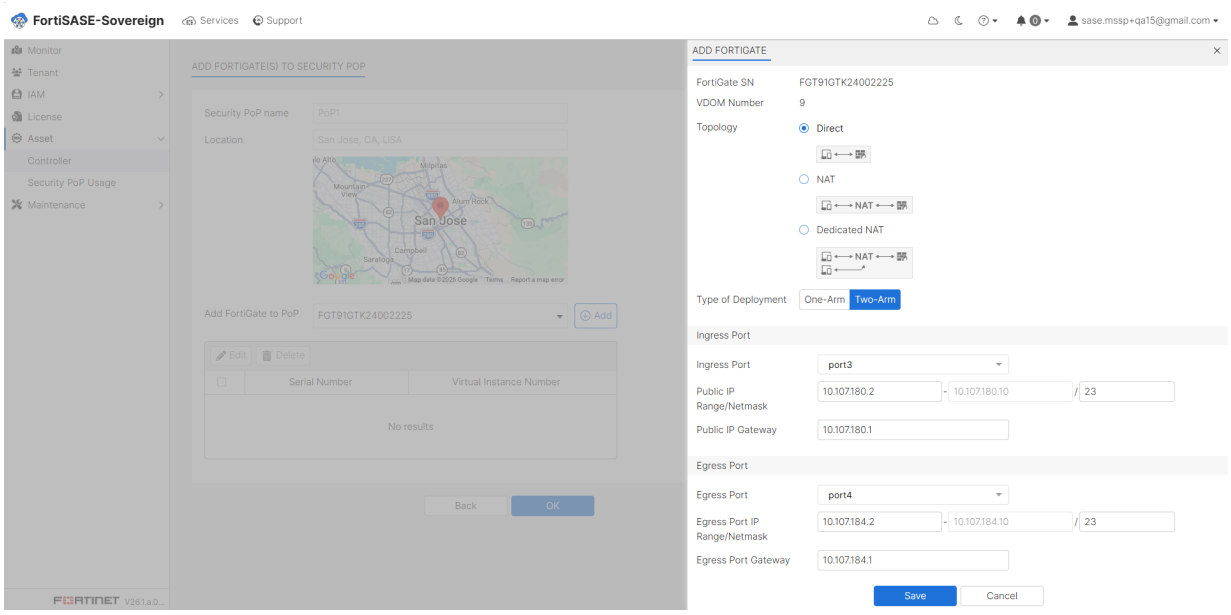


4. To add a FortiGate to a Security PoP, click +New FortiGate and proceed with the configuration steps outlined below. If you wish to complete the initial controller onboarding without adding a FortiGate at this

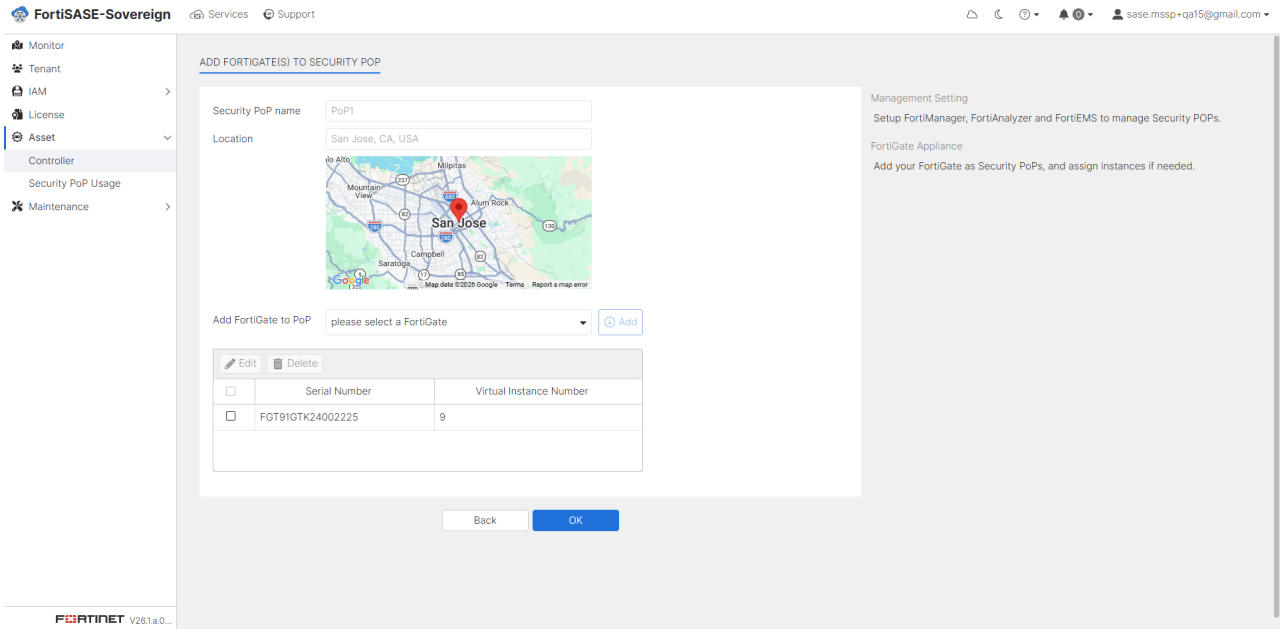
stage, click Skip. FortiGate devices can be added or modified at any time after the onboarding process is complete.



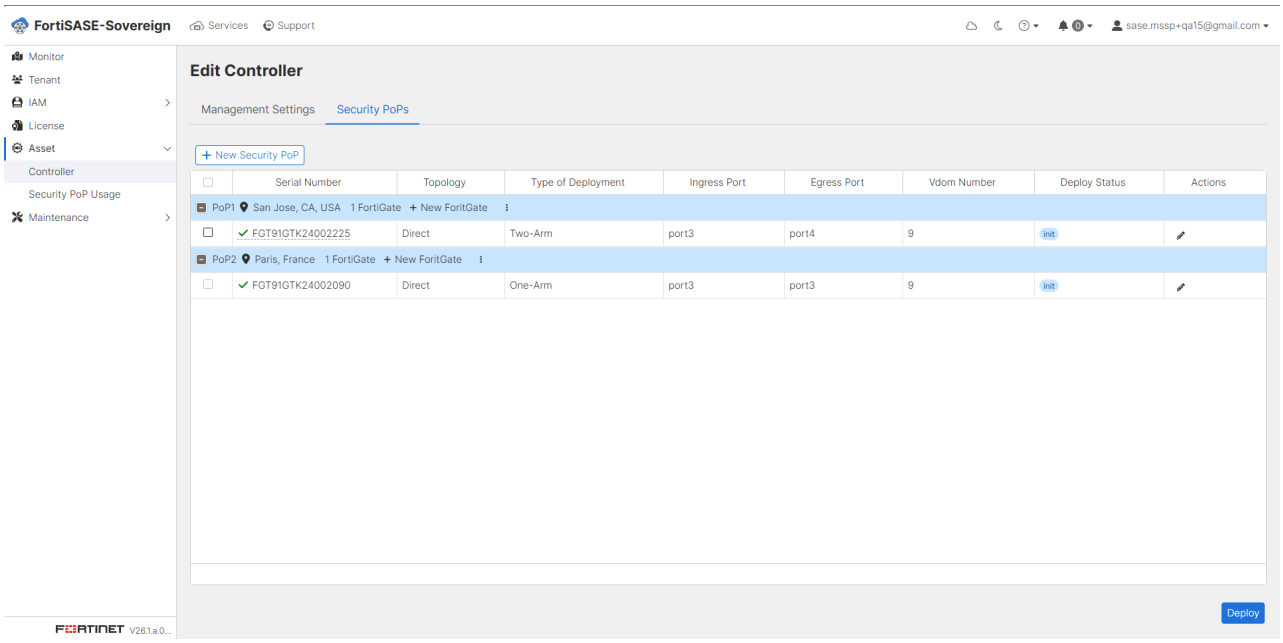
5. Configure the Security Point of Presence (PoP) by providing the Security PoP Name and physical or logical Location, then select the FortiGate device(s) to be assigned to this PoP. Each Security PoP represents a logical enforcement point through which tenant traffic is inspected and secured. Configure the FortiGate using the following steps:
   a. Open the ADD FORTIGATE panel and verify the FortiGate Serial Number (SN) and the designated VDOM Number to ensure the correct appliance is being registered.
   b. Select the appropriate network Topology from the three available options — Direct, NAT, or Dedicated NAT — based on your network architecture and traffic routing requirements.
   c. Select the Type of Deployment that best suits your network design. Two deployment modes are available:
      - Two-Arm: Utilizes separate, dedicated interfaces for ingress and egress traffic, providing enhanced traffic isolation and granular policy enforcement at each network boundary.
      - One-Arm: Employs a single shared interface for both traffic directions, commonly used in environments that require inline inspection with centralized routing separation.
   d. Configure the Ingress Port by specifying the network interface parameters through which inbound tenant traffic will enter the FortiGate appliance for inspection and policy enforcement.
   e. Configure the Egress Interface by defining the outbound network interface parameters through which processed traffic will exit the FortiGate appliance toward its destination.
   f. Review the configuration, and then click Save to commit the FortiGate settings to the controller. The system will validate the configuration before finalizing the registration.



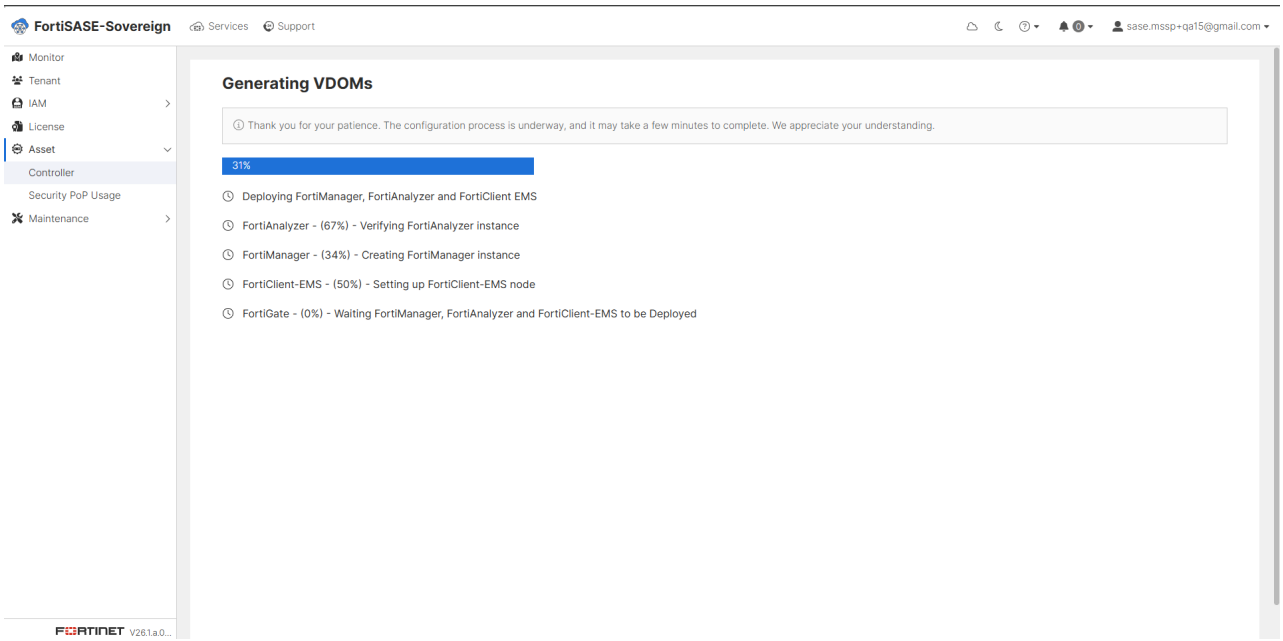
6. Review the FortiGate configuration summary presented in the confirmation dialog. Once all parameters have been verified as correct, click OK to finalize the FortiGate registration and associate the appliance with the designated Security PoP.



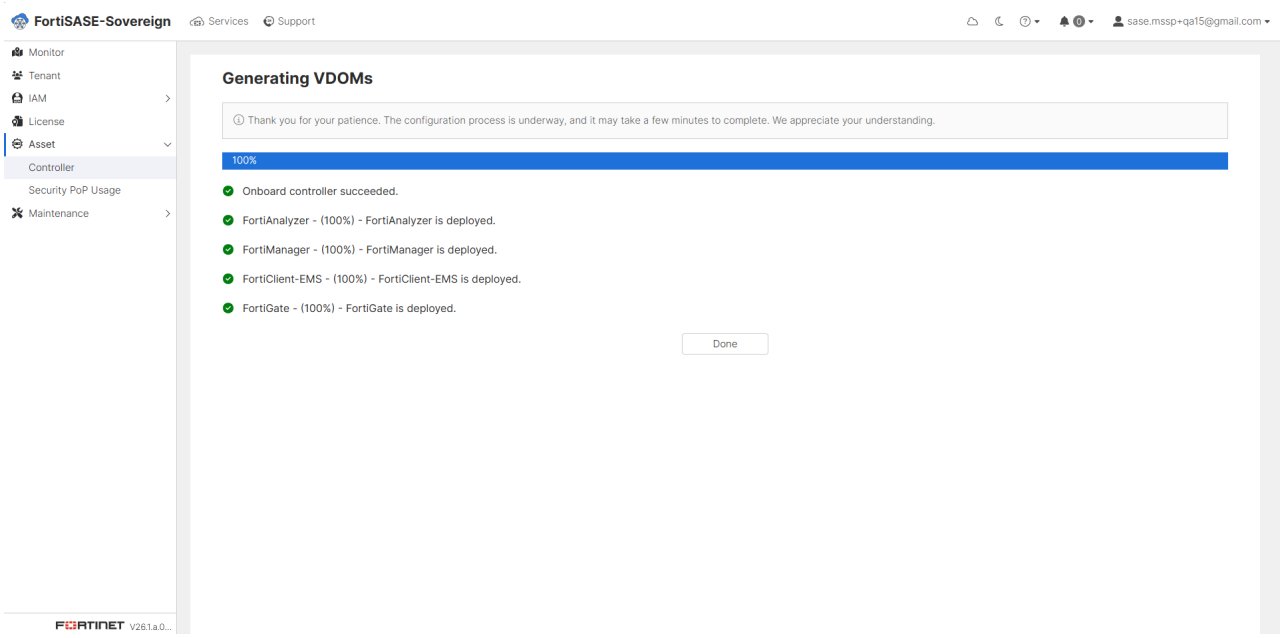
7. Review the Security PoP summary to confirm that all FortiGate appliances have been successfully registered and are displaying an Init Deploy Status, indicating they are ready for provisioning. Once the configuration has been verified, click Deploy to initiate the automated onboarding process and begin VDOM generation across all registered FortiGate devices.



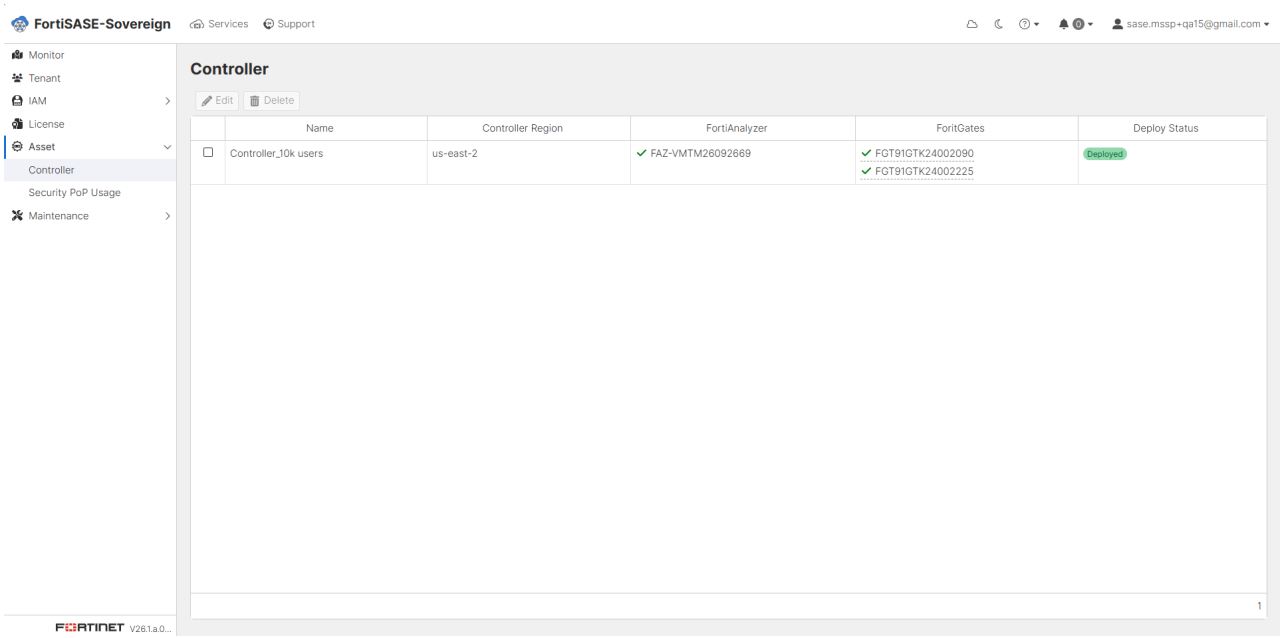
8. Monitor the deployment progress on the Generating VDOMs page. Each VDOM provisioning task will display its current status as the system automatically configures virtual domains across all associated FortiGate appliances. This also includes FortiManager, FortiAnalyzer and FortiClient EMS deployment. It is suggested do not navigate away from this page while the deployment is in progress.



9. When deployment reaches 100% and the system confirms Onboard controller succeeded click Done to exit the deployment wizard. The controller is now fully provisioned and operational within the Multi-Tenant Instance.

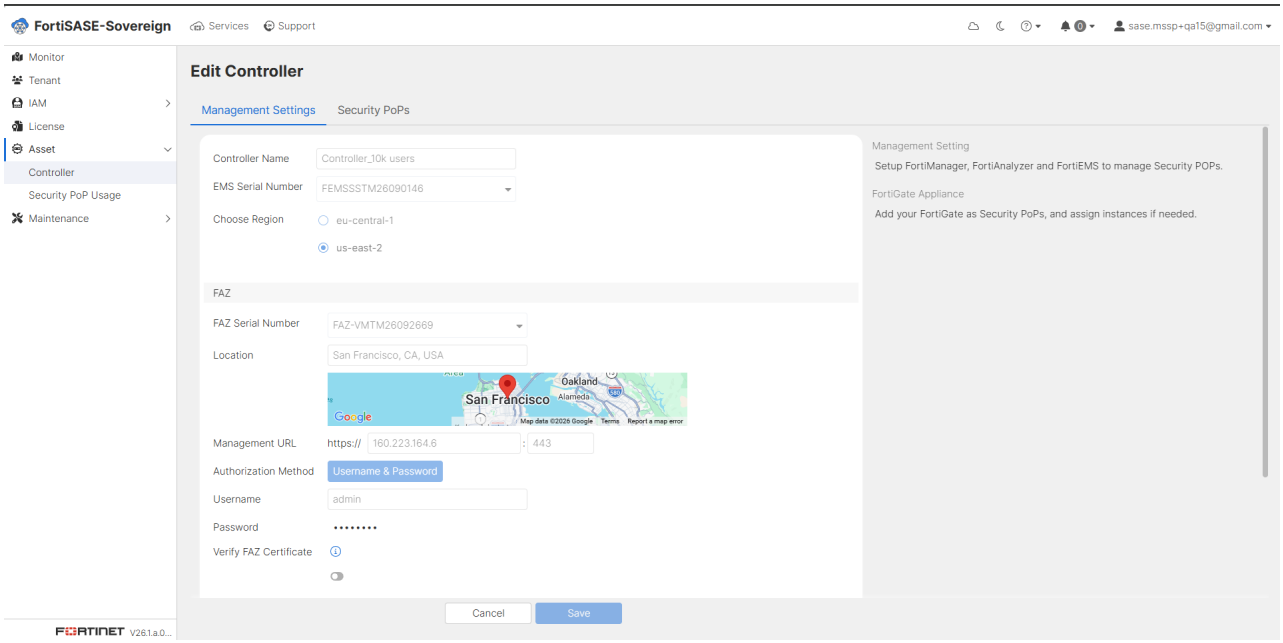


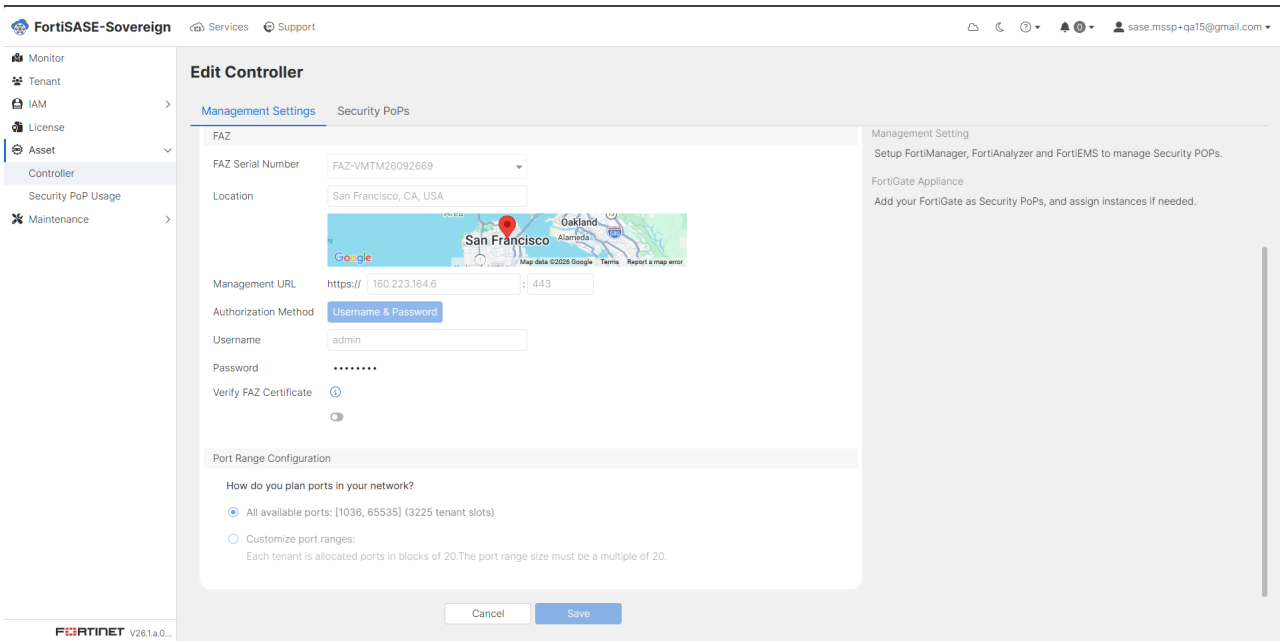
10. Return to the Asset Controller dashboard to verify that the newly provisioned controller is listed with Deployed status. Confirm that all associated FortiGate appliances, Security PoP configurations, and VDOM assignments are accurately reflected in the system. The Multi-Tenant Instance Controller Onboarding process is now complete and the environment is ready for Tenant Onboarding.



Controller Management

1. Select the desired controller from the list, Click Edit Controller to open the configuration page, select the Management Settings tab to view all controller related configurations.





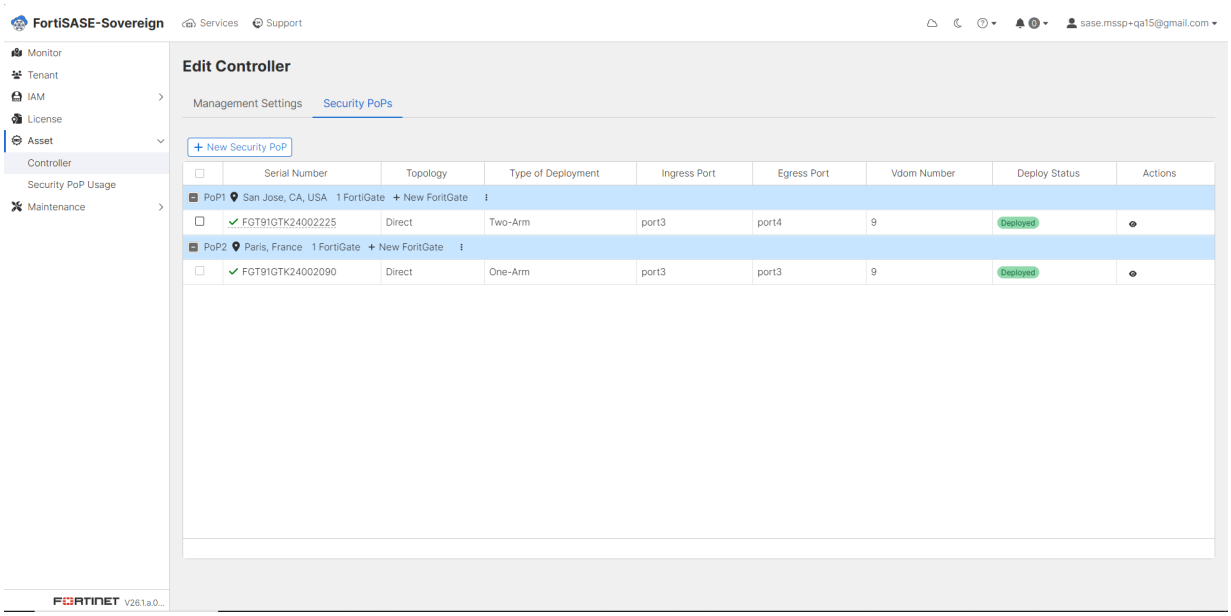
2. Click Security PoPs tab to manage Security PoPs.
   a. Add a New Security PoP.
      i. Click + New Security PoP to initiate the PoP creation workflow.
      ii. Configure FortiGate device details, topology, deployment type, and interface mappings.
   b. View Existing PoP Details

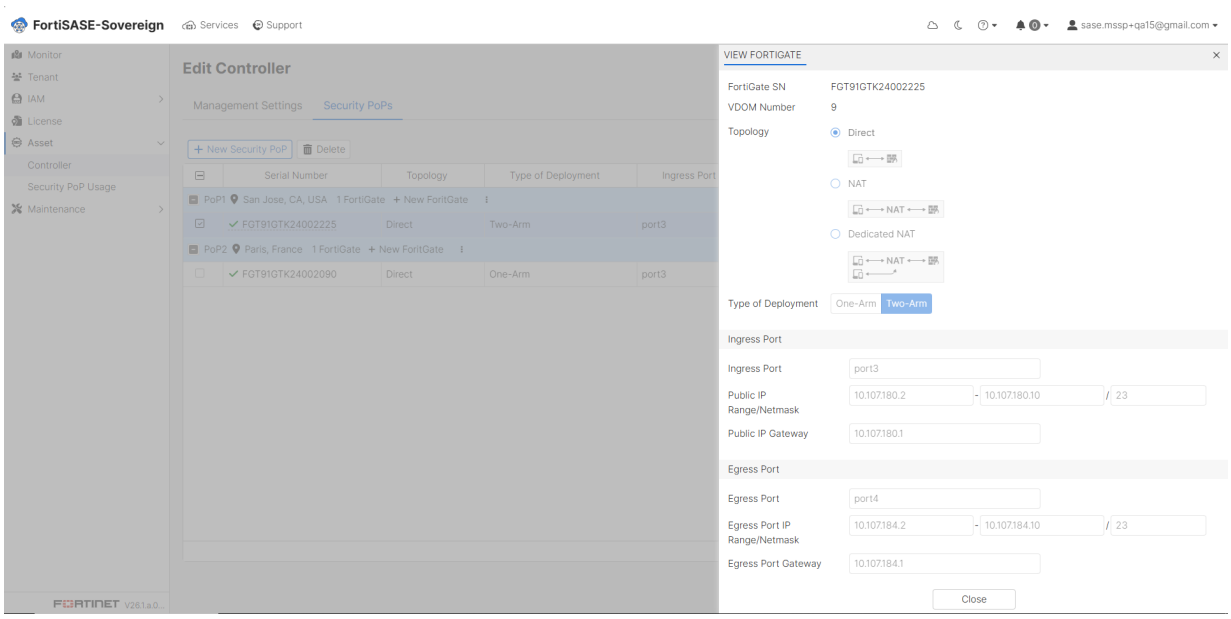
i. Expand a PoP entry to view associated FortiGate devices.
ii. Review configuration details such as topology, ports, and VDOM assignments.

c. Verify Deployment Status
   i. Ensure each PoP shows a Deployed status.
   ii. A deployed state indicates successful provisioning and readiness for traffic handling.

d. Validate Interface Configuration
   - Confirm that Ingress and Egress ports are correctly mapped based on deployment type:
     - Two-Arm: Separate ingress and egress interfaces (e.g., port3 → port4).
     - One-Arm: Same interface used for both directions (e.g., port3 → port3).

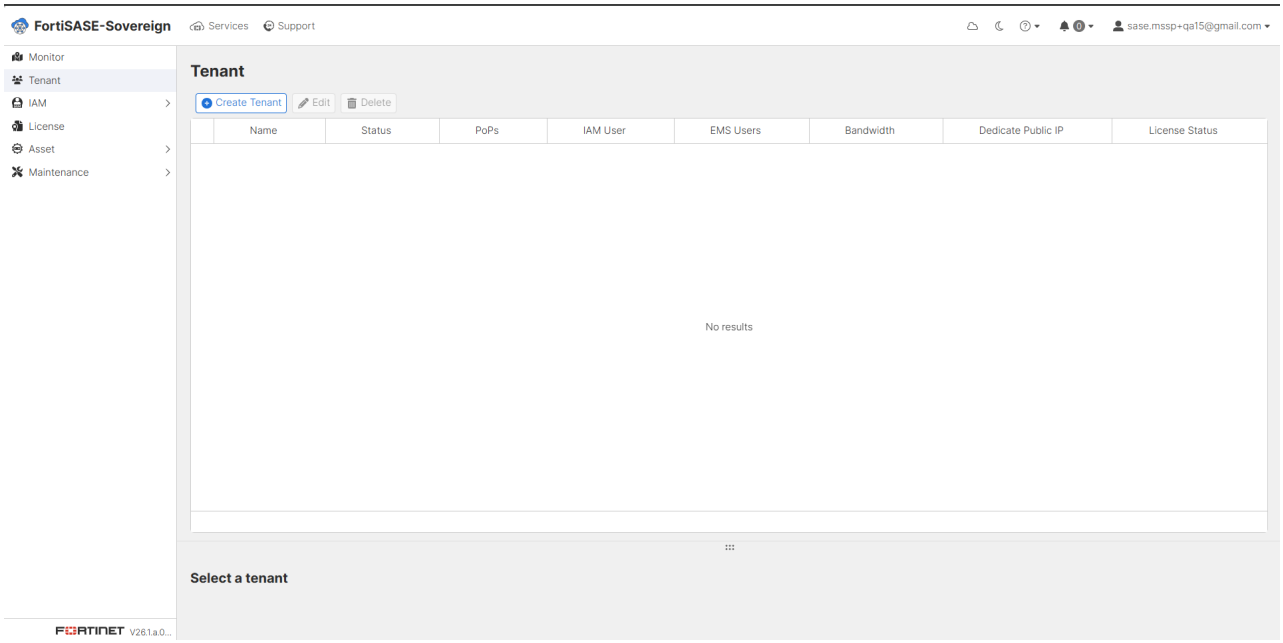
e. Check Multi-Region Deployment
   - Verify PoPs across different geographic locations (e.g., San Jose, Paris) to ensure global coverage and redundancy.



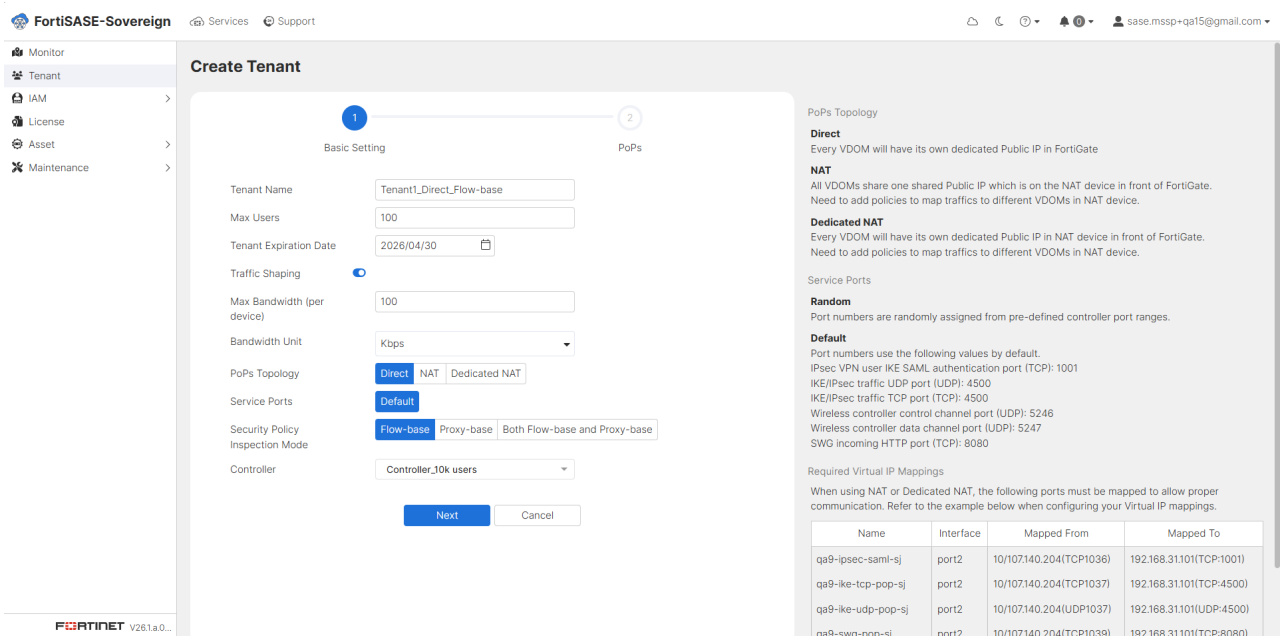


Tenant Onboarding

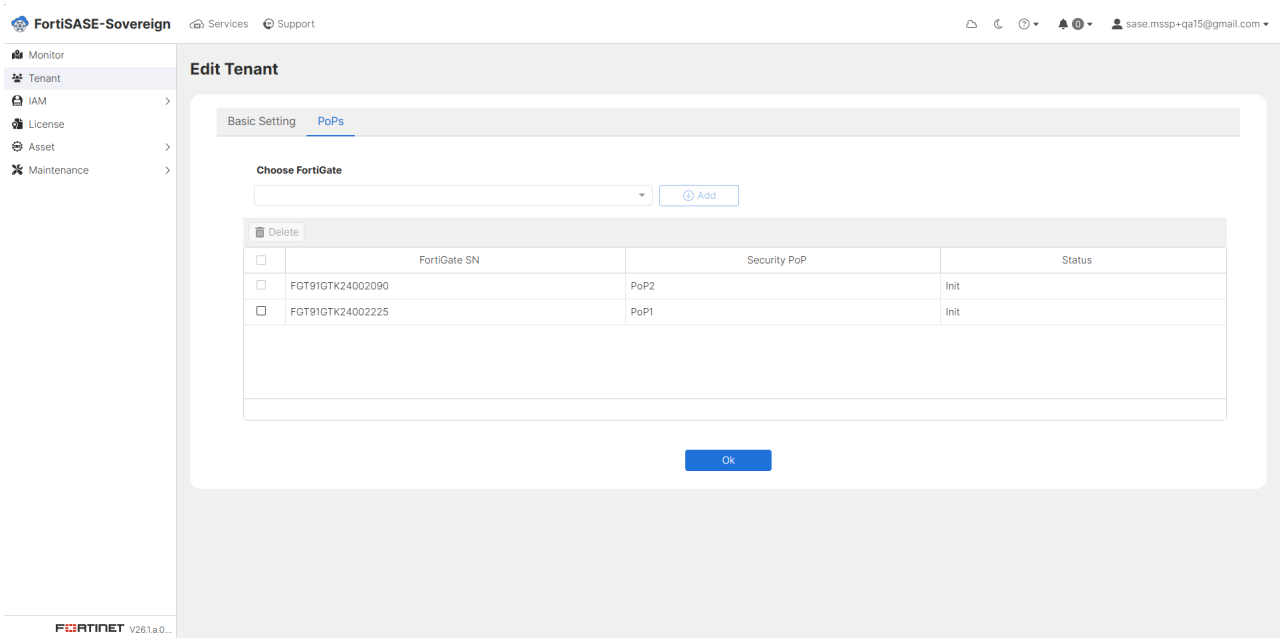
1. Go to the Tenant section. The tenant list will display No results when no tenants have been provisioned. Click Create Tenant to begin onboarding a new managed tenant environment under the MSSP controller.



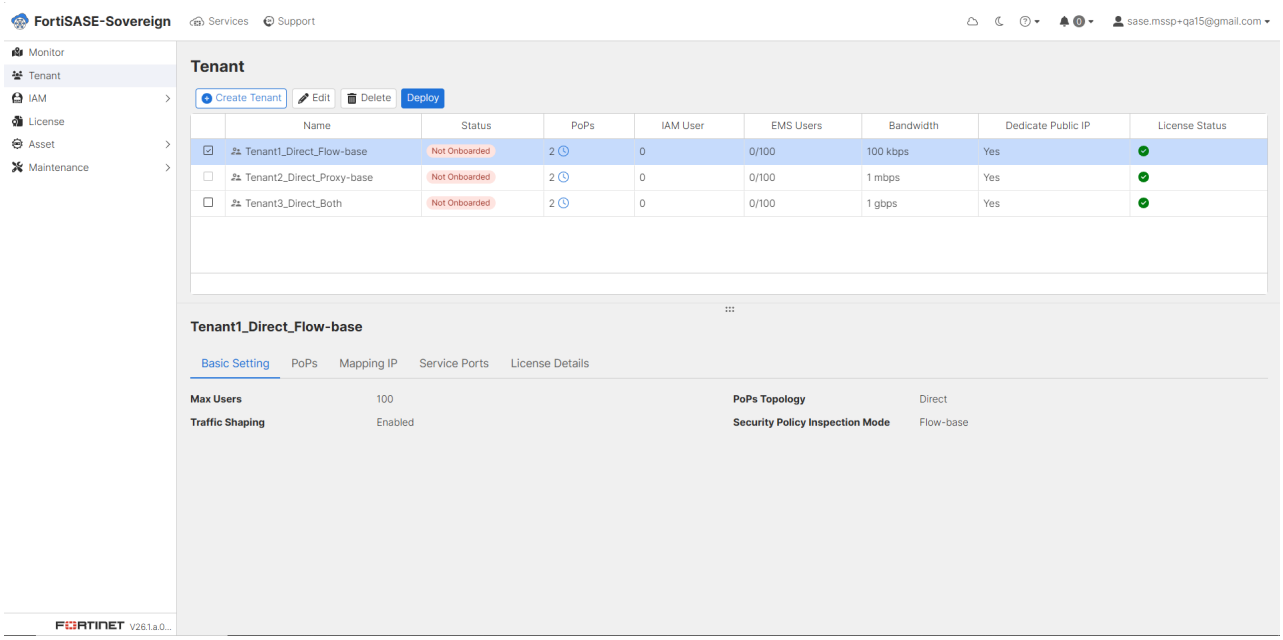
2. Fill in the basic tenant settings. Enter a descriptive Tenant Name, specify the maximum number of licensed user seats (Max Users), and set the Tenant Expiration Date. Enable Traffic Shaping if bandwidth management is required and configure the Max Bandwidth (per device) and Bandwidth Unit accordingly. Select the PoPs Topology (Direct, NAT, or Dedicated NAT), choose the Service Ports allocation method (Random or Default), and set the Security Policy Inspection Mode (Flow-base, Proxy-base, or Both Flow-base and Proxy-base). Finally, assign the appropriate Controller. The right-hand panel provides topology descriptions and required Virtual IP mappings for reference. Click Next to proceed to the PoPs assignment step.



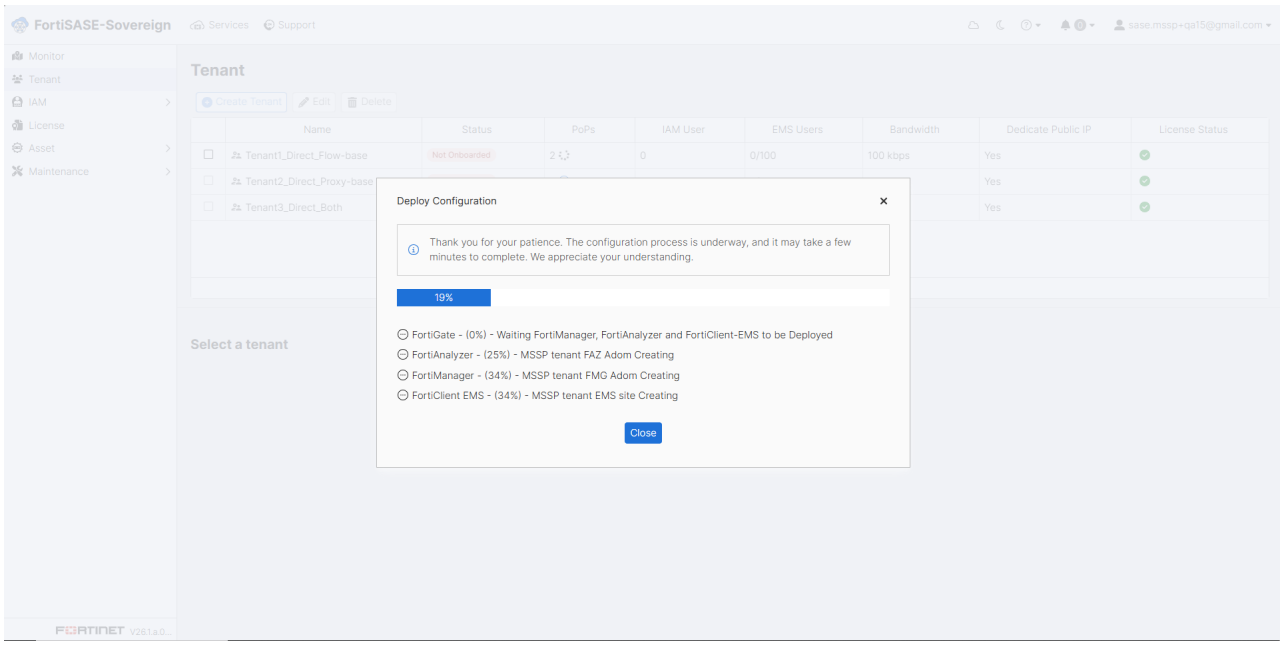
3. In the PoPs assignment step, use the Choose FortiGate dropdown to select the FortiGate appliances to associate with this tenant. The table displays each FortiGate Serial Number, its assigned Security PoP, and the current initialization status. Once all desired FortiGate devices have been added, click OK to confirm the PoP assignment and complete the tenant creation.



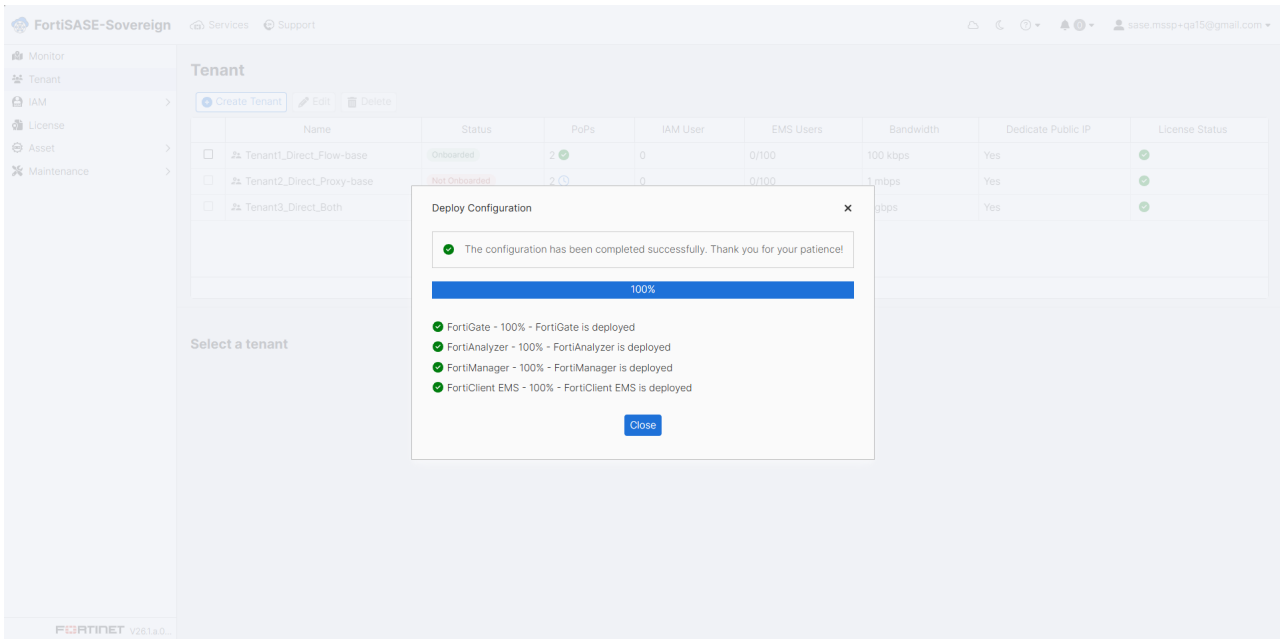
4. After creating tenants, the Tenant list displays all provisioned tenants showing each tenant's Name, Status, PoPs count, IAM User count, EMS Users, Bandwidth, Dedicated Public IP assignment, and License Status. Newly created tenants will show a Not Onboarded status, indicating they are pending deployment. Select one or more tenants and click Deploy to initiate the automated provisioning process for the selected tenant environments.



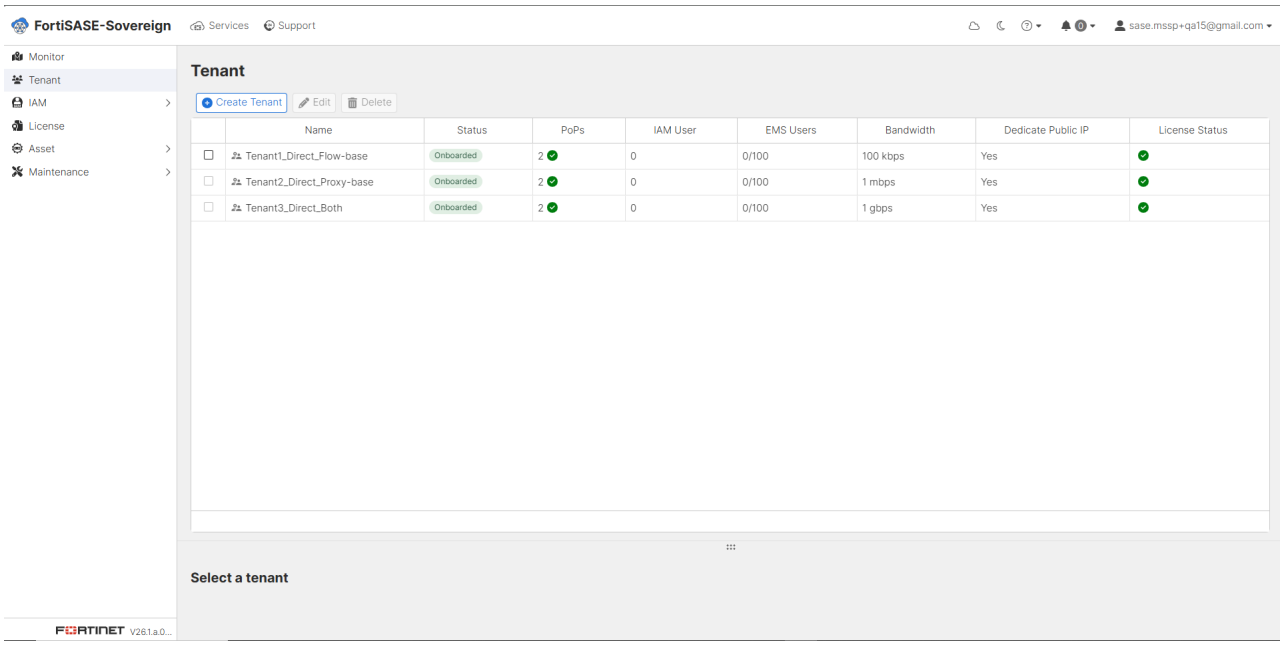
5. After clicking Deploy, the Deploy Configuration dialog appears and shows real-time provisioning progress. The system sequentially deploys FortiGate, FortiAnalyzer, FortiManager, and FortiClient EMS components for the tenant. Each component displays its current progress percentage and task description. Clicking Close can close this dialog while provisioning is in progress background.



6. When all components have reached 100% and the dialog confirms “The configuration has been completed successfully,” click Close to dismiss the Deploy Configuration dialog. All four components — FortiGate, FortiAnalyzer, FortiManager, and FortiClient EMS — should display a fully deployed status before proceeding.



7. Return to the Tenant list to verify that all deployed tenants now display an Onboarded status with a green indicator. Confirm that each tenant's PoP count, Bandwidth allocation, Dedicate Public IP assignment, and License Status are accurately reflected. The tenant onboarding process is now complete and each tenant environment is ready for end-user connectivity and policy configuration.

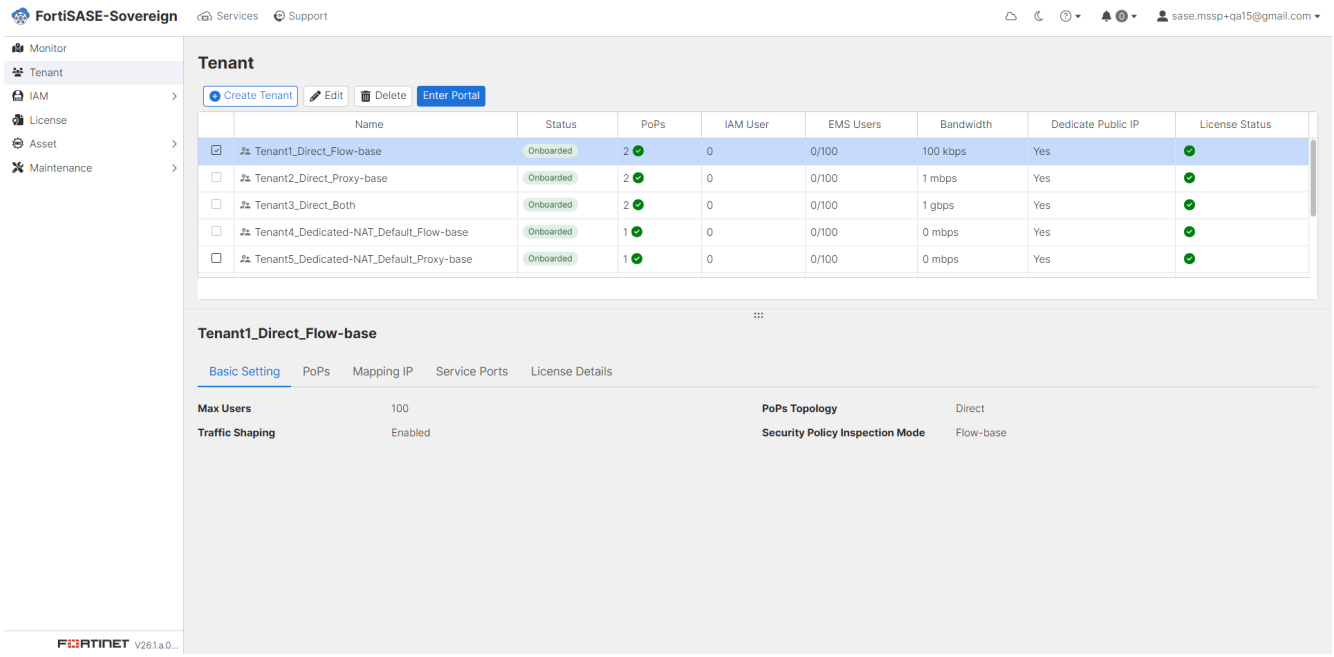


Tenant Management

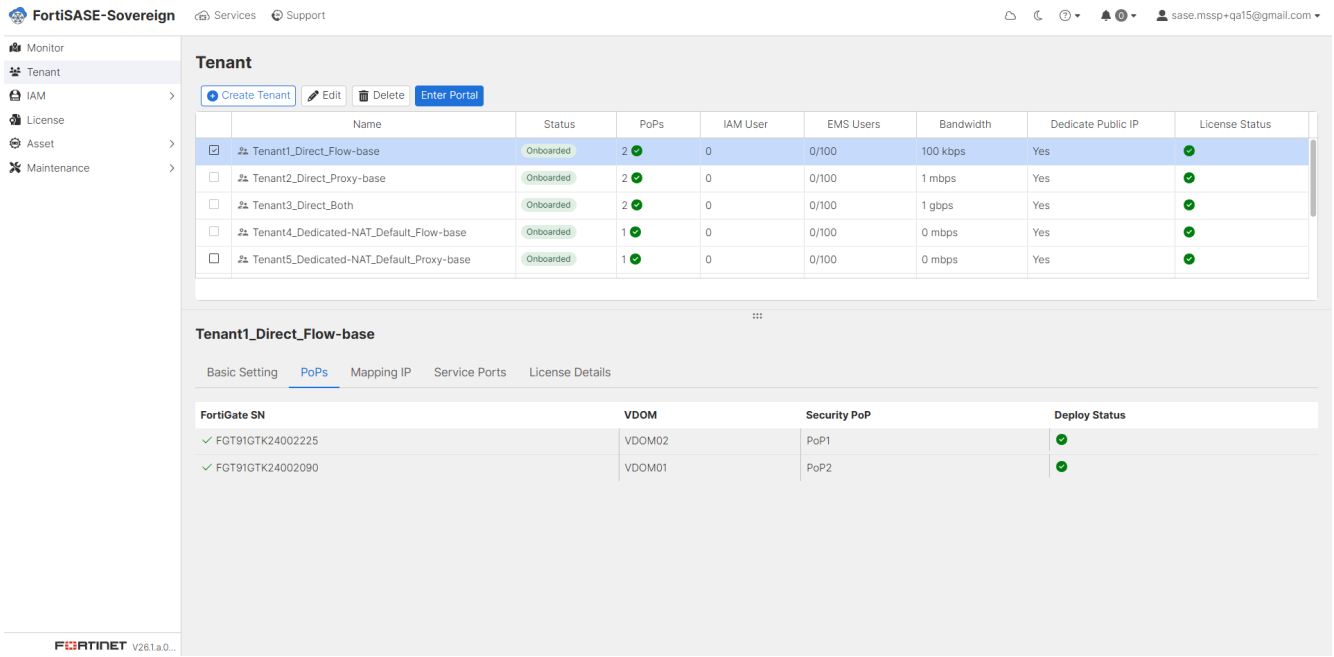
The Tenant Management section allows administrators to manage tenants over tenant environments. From this view, MSSP administrators can create new tenants, modify existing tenant configurations via the Edit action, or permanently remove a tenant using the Delete option. Each listed tenant can be individually selected to reveal detailed configuration tabs in the panel below.

To access a tenant's dedicated management portal, select the tenant from the list and click Enter Portal. This launches the tenant-scoped interface, where administrators can manage security policies, device configurations, and monitoring dashboards specific to that tenant environment.

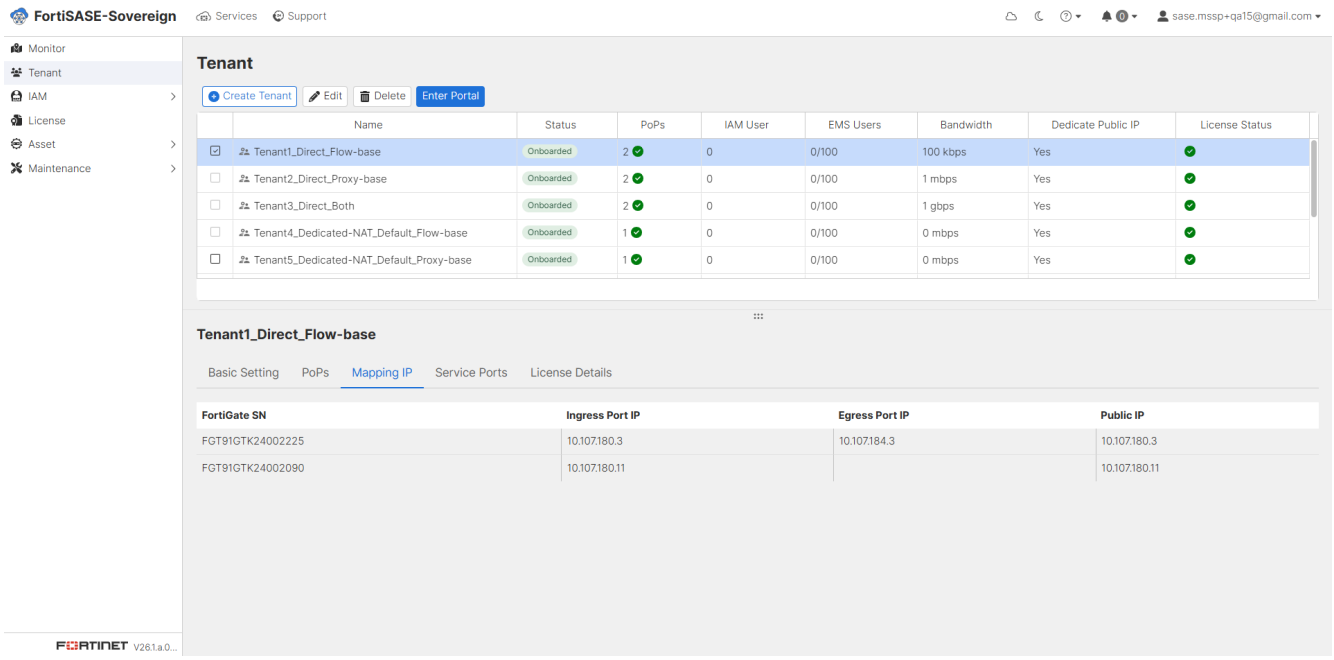
Select a tenant from the list to display its Basic Setting details in the lower panel. The Basic Setting tab provides a summary of the tenant's core configuration parameters, including the maximum licensed user count (Max Users), Traffic Shaping status, PoPs Topology type, and the configured Security Policy Inspection Mode. This tab serves as the primary reference for validating the tenant's foundational deployment parameters.



Select a tenant and navigate to the PoPs tab to display all Security Points of Presence associated with that tenant. The table lists each assigned FortiGate SN (Serial Number), its corresponding VDOM identifier, the linked Security PoP name, and the current Deploy Status. A green indicator confirms that the FortiGate is successfully deployed and actively enforcing traffic policies for the tenant.

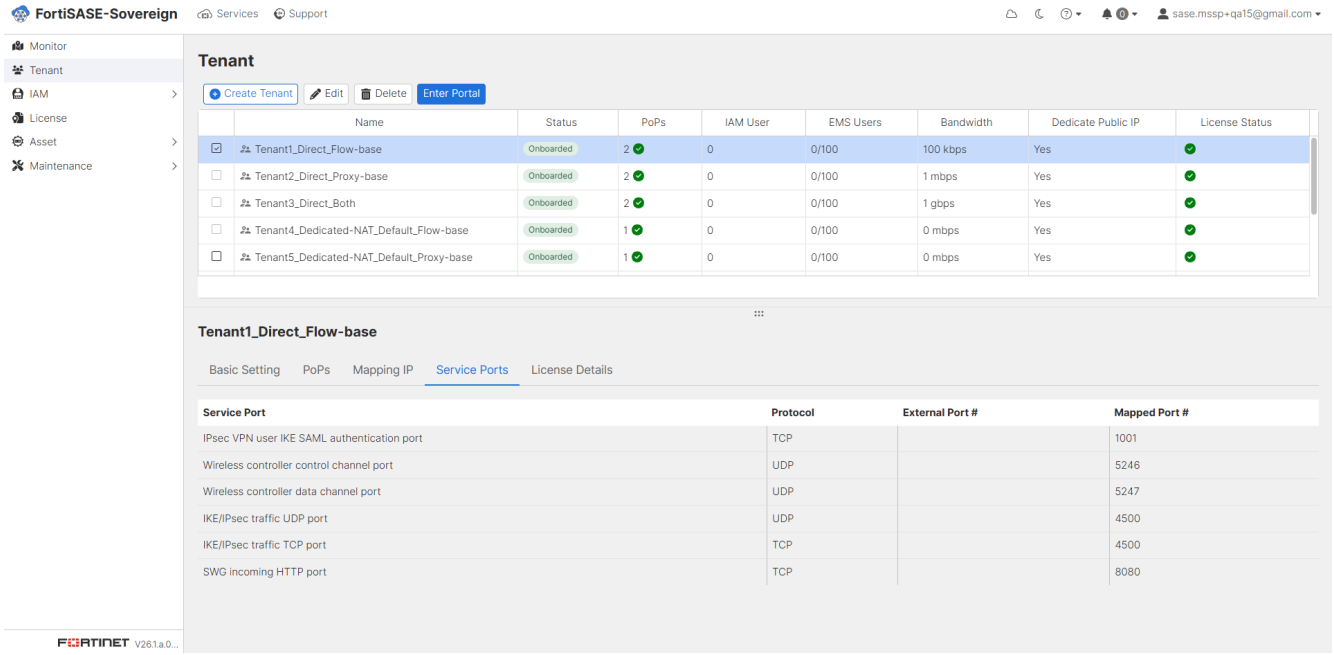


Select a tenant and navigate to the Mapping IP tab to view the IP address assignments for each FortiGate appliance associated with that tenant. The table displays each FortiGate SN (Serial Number) alongside its Ingress Port IP, Egress Port IP, and the assigned Public IP address. This information is essential for verifying correct traffic routing and for configuring upstream firewall or NAT rules that direct tenant traffic to the appropriate FortiGate interfaces.



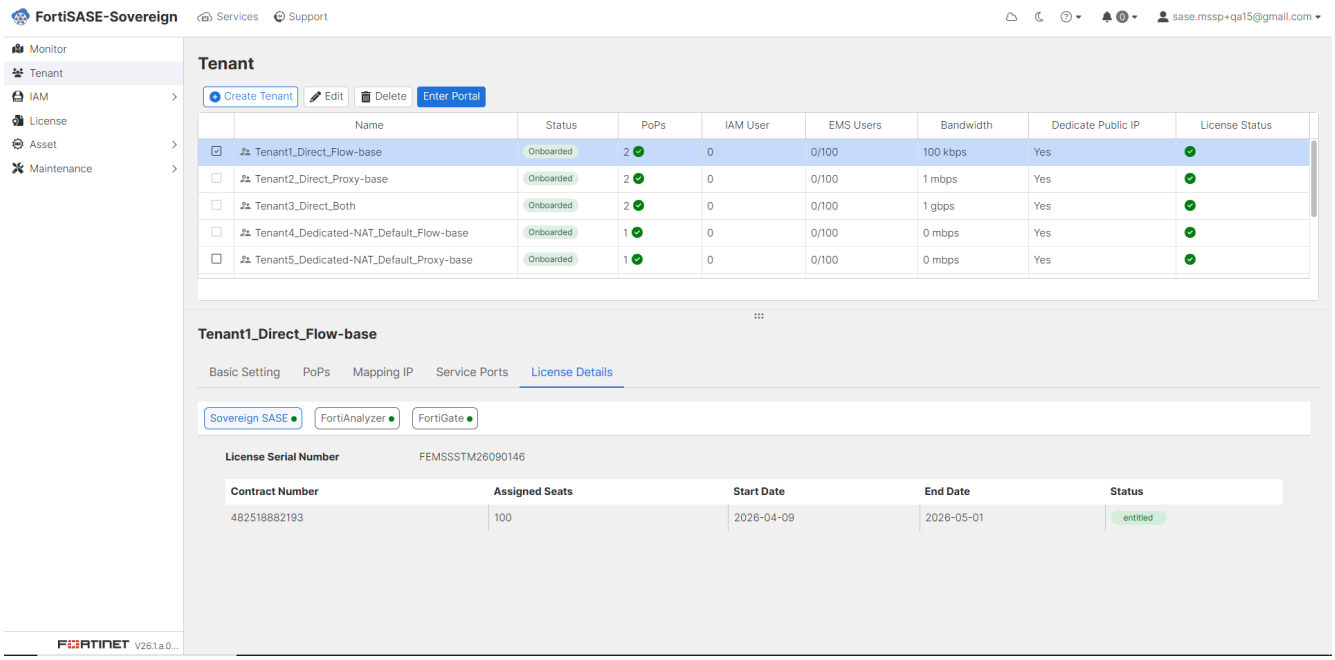
Select a tenant and navigate to the Service Ports tab to review the port mappings that govern tenant service connectivity. The table lists each Service Port by name (such as IPsec VPN, Wireless controller, IKE/IPsec traffic, and SWG Incoming HTTP), its Protocol (TCP or UDP), the External Port number exposed to tenant users, and the

internally Mapped Port number used within the FortiGate VDOM. These mappings must align with the Virtual IP configurations applied to the FortiGate to ensure uninterrupted service delivery.

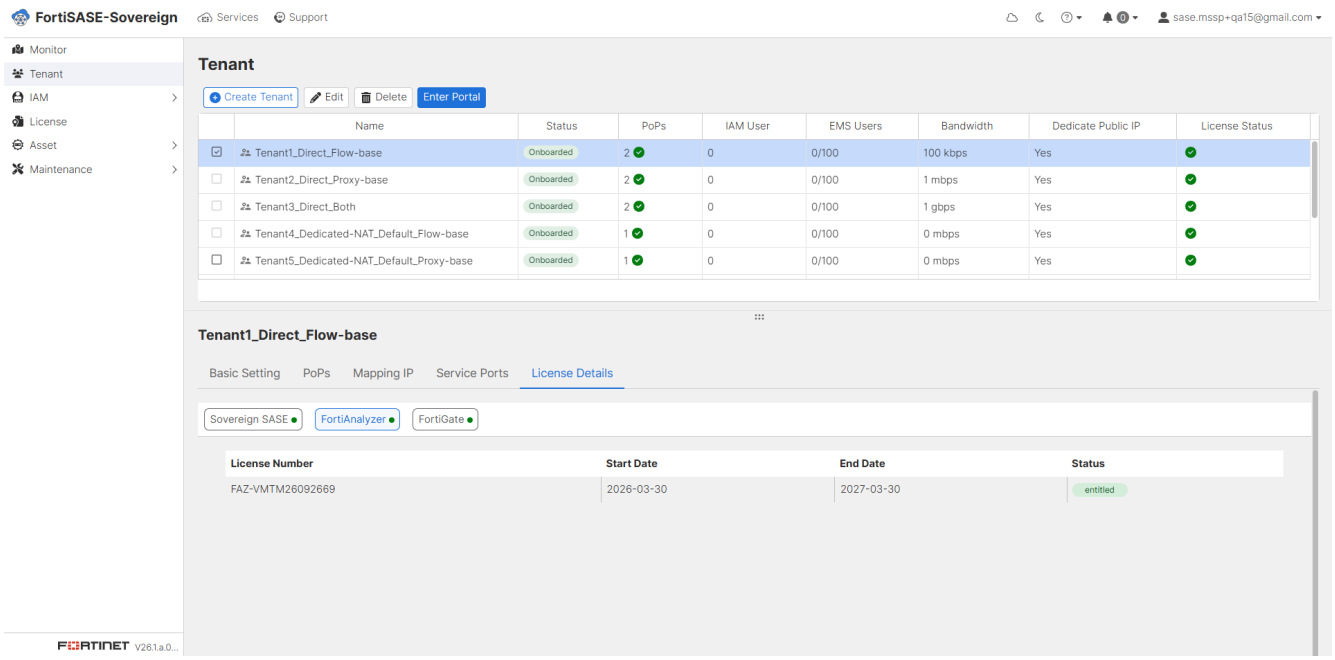


Select a tenant and navigate to the License Details tab to review all active license entitlements associated with that tenant. The tab is organized into three sub-tabs — Sovereign SASE, FortiAnalyzer, and FortiGate — each displaying the relevant license serial numbers, contract details, assigned seat counts, validity dates, and current activation status.

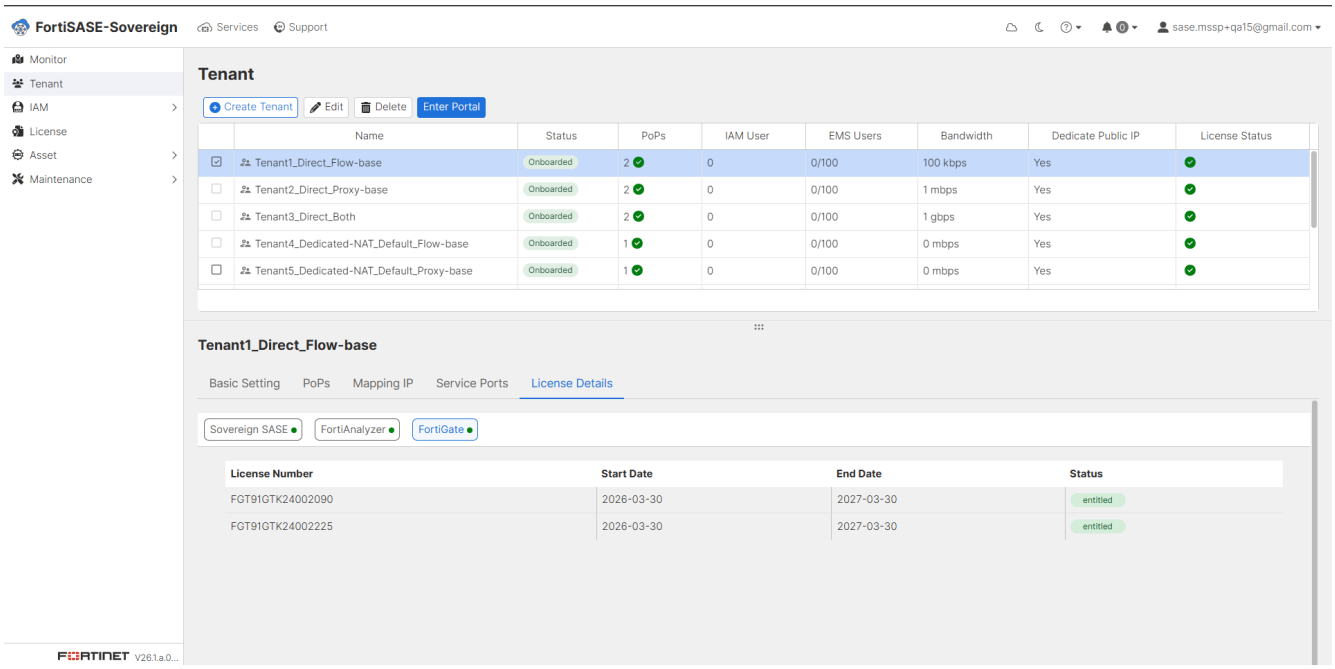
The Sovereign SASE sub-tab displays the FortiClient EMS license details provisioned for this tenant. The table shows the License Serial Number, associated Contract Number, the number of Assigned Seats, the contract Start Date, End Date, and current activation Status. Verify that the license status shows entitled and that the seat count and validity period align with the tenant's service agreement before granting end-user access.



The FortiAnalyzer sub-tab displays the log management and analytics license associated with this tenant's FortiAnalyzer instance. The table lists the License Number, contract Start Date, End Date, and activation Status. Confirm the license is entitled status and within its validity period to ensure uninterrupted log collection, event correlation, and compliance reporting for the tenant.

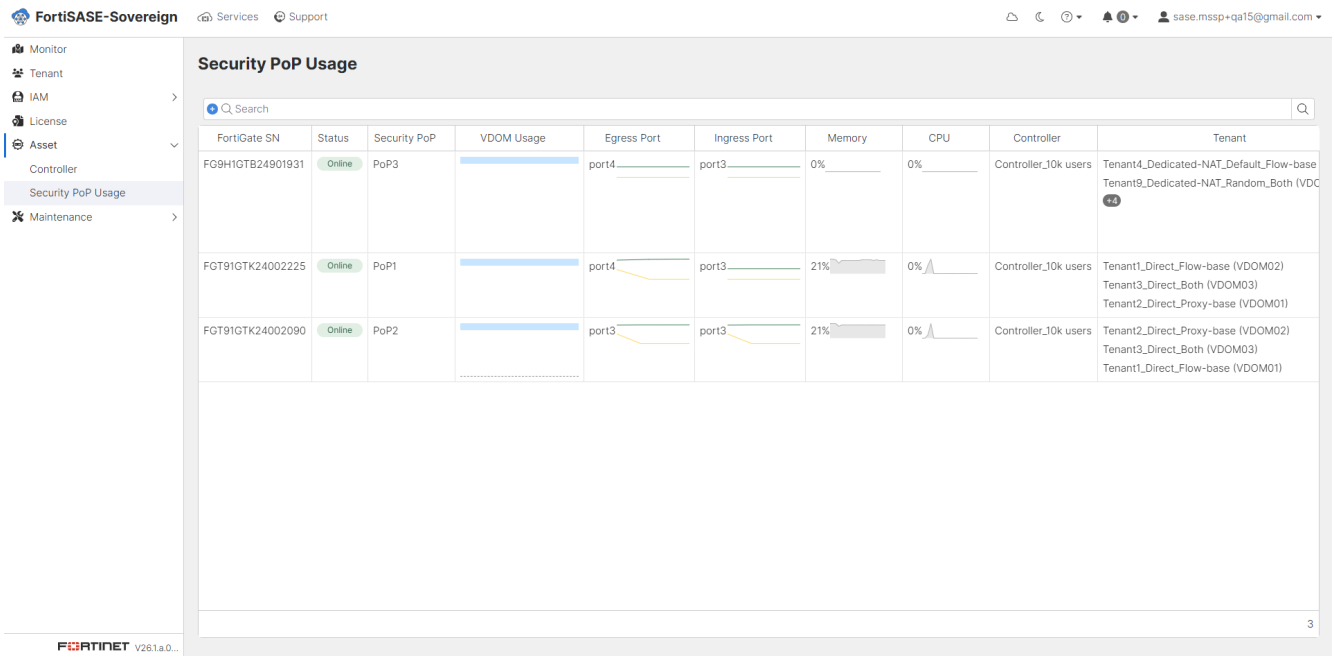


The FortiGate sub-tab lists the individual FortiGate appliance licenses assigned to this tenant. Each row displays the License Number corresponding to a specific FortiGate Serial Number, along with the contract Start Date, End Date, and current activation Status. Verify that all FortiGate licenses are showing an entitled status and that their validity periods cover the full term of the tenant's service contract.



Security PoP Usage

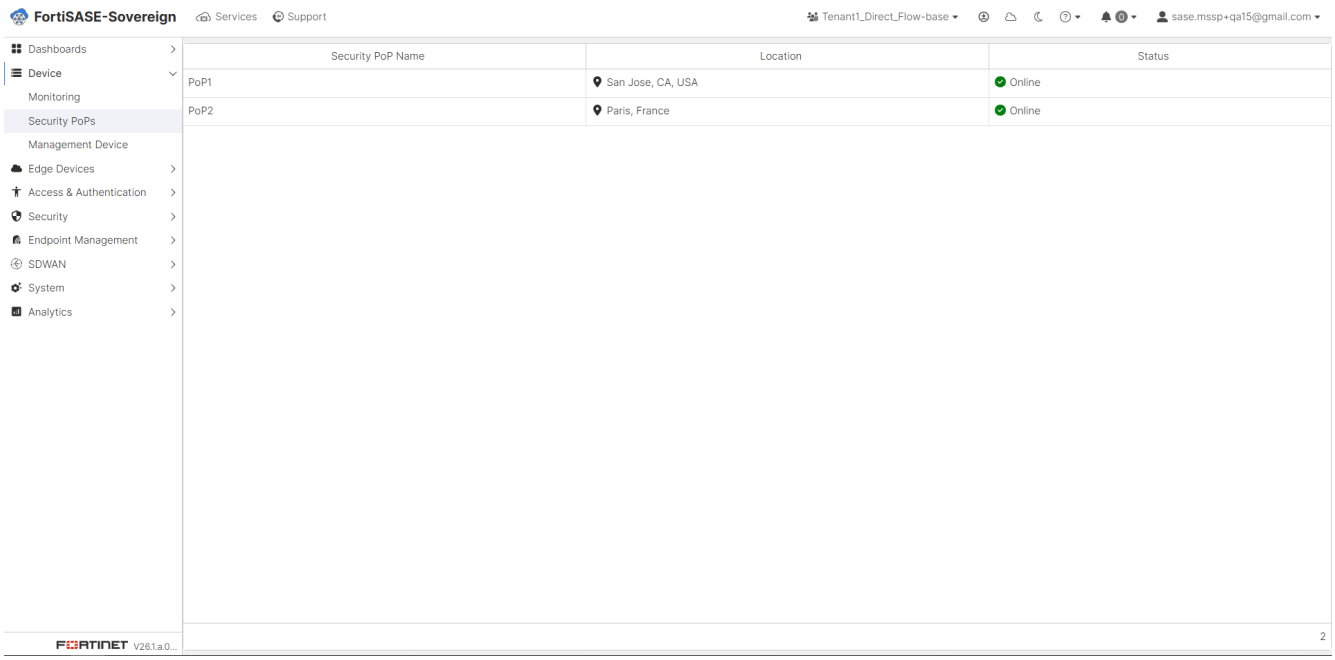
The Security PoP Usage dashboard, accessible from Asset > Security PoP Usage, provides a consolidated, real-time operational view of all FortiGate appliances across every registered Security PoP. Each row represents a FortiGate device and displays its Serial Number, online Status, assigned Security PoP name, VDOM Usage bar, Egress Port, Ingress Port, Memory utilization, CPU load, associated Controller, and the list of Tenant VDOMs currently hosted on that appliance. This view is the primary resource for monitoring hardware resource consumption, validating tenant VDOM distribution across PoPs, and identifying any FortiGate appliances that may require capacity attention.



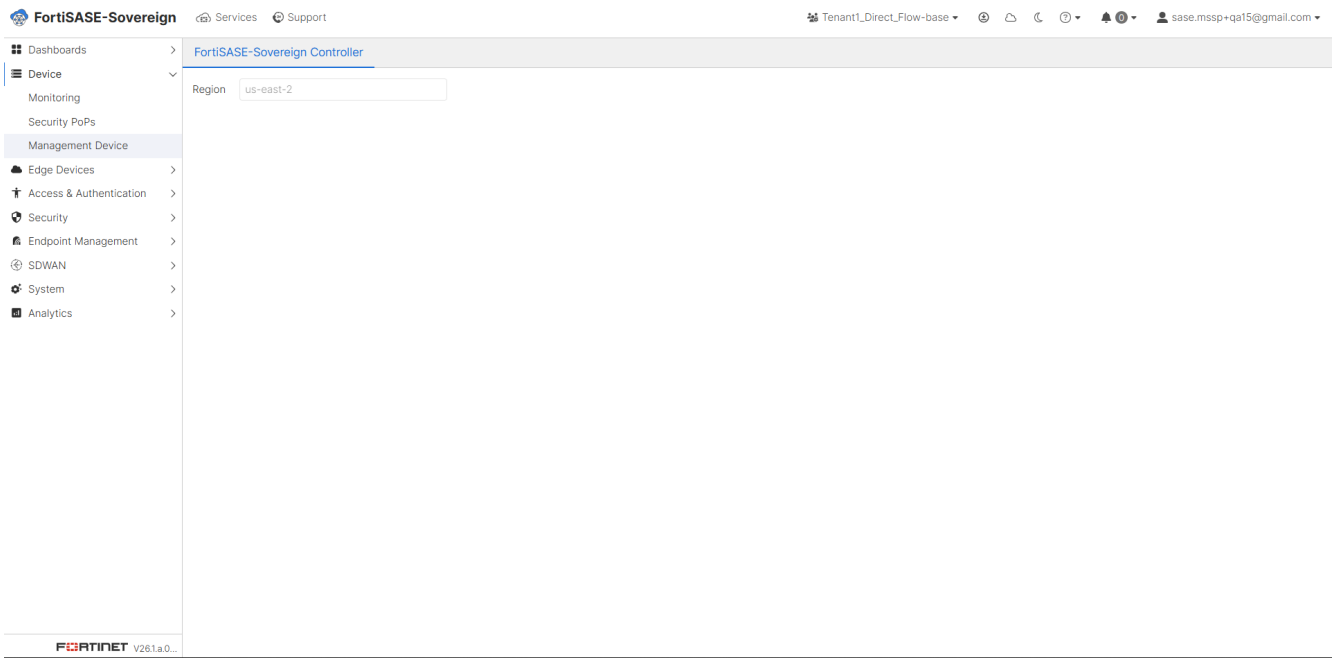
Tenant Portal Device Management

Within each tenant's dedicated portal, the Device section provides tenant-level visibility and management of the infrastructure components assigned to that environment. This section is divided into two sub-pages: Security PoPs and Management Device, both accessible under Device in the tenant portal navigation.

Security PoPs Management: The Security PoPs sub-page within the tenant portal displays all Security Points of Presence assigned to the tenant, along with their geographic Location and current operational Status. Each PoP entry shows the Security PoP Name, its physical or logical deployment Location (e.g., San Jose, CA, USA or Paris, France), and an Online/Offline Status indicator confirming active enforcement. Administrators can use this view to verify that all assigned PoPs are reachable and operational before rolling out end-user connectivity.



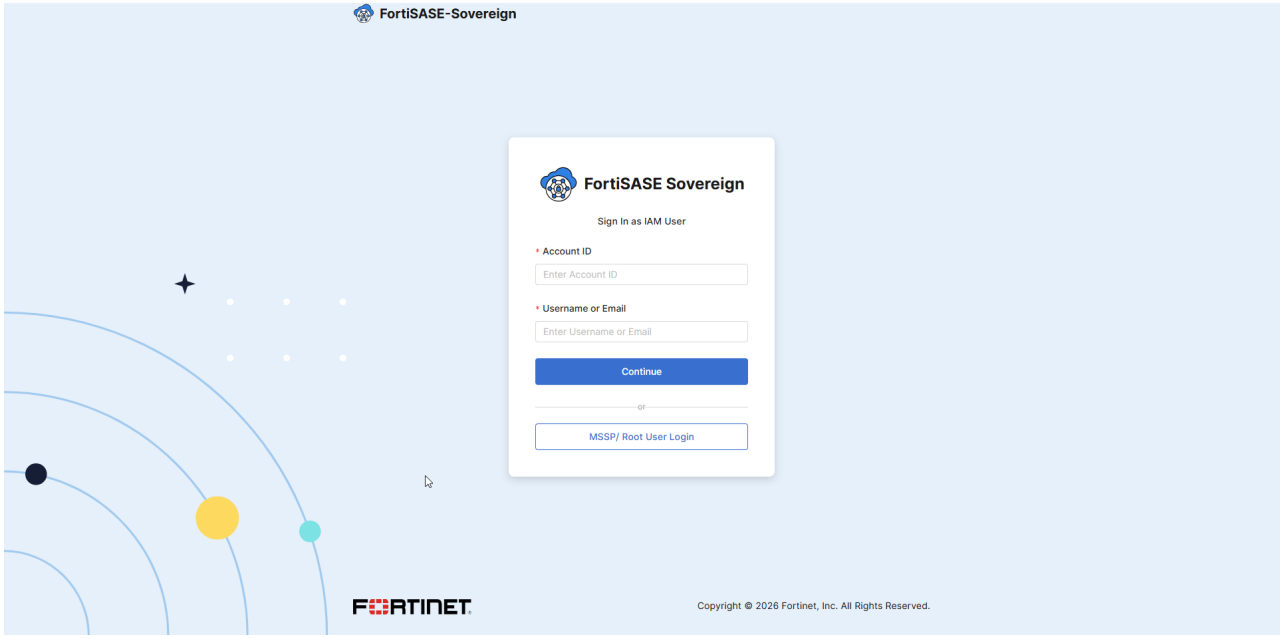
Management Device: The Management Device sub-page displays the FortiSASE-Sovereign Controller instance associated with the tenant. This view confirms the controller Region assignment and provides a reference point for the management plane infrastructure serving the tenant environment. Administrators can use this page to confirm that the tenant is associated with the expected regional controller. Ensure the displayed region matches the intended deployment location.



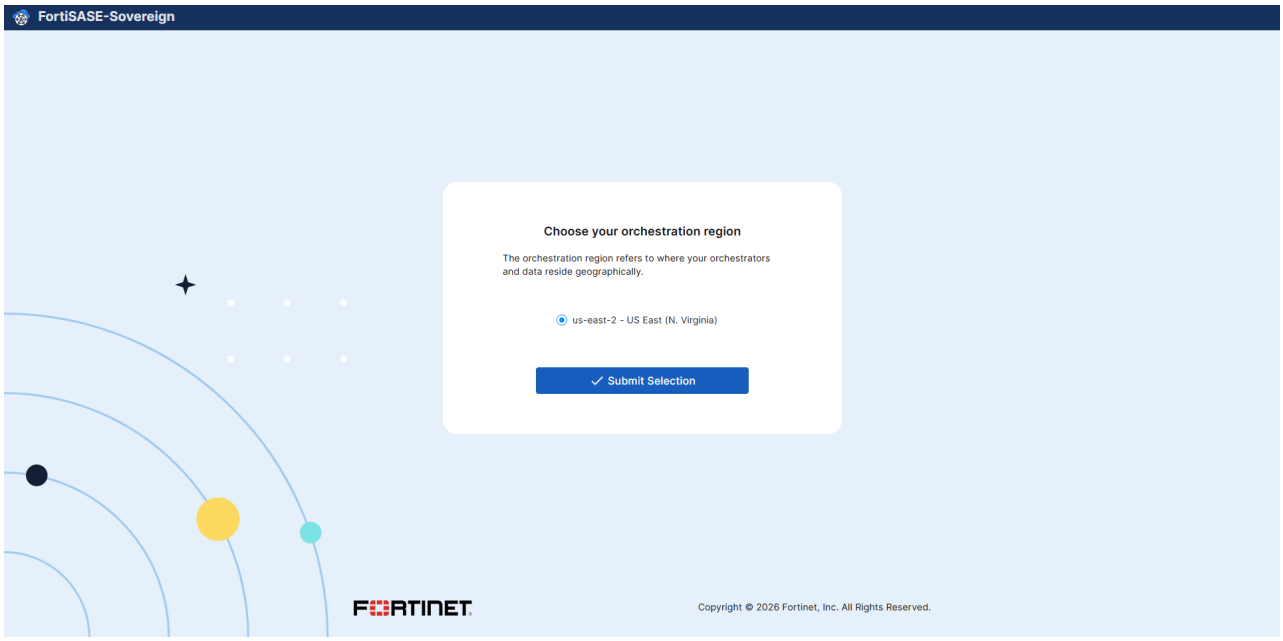
Single Tenancy Onboarding

Login Landing Page

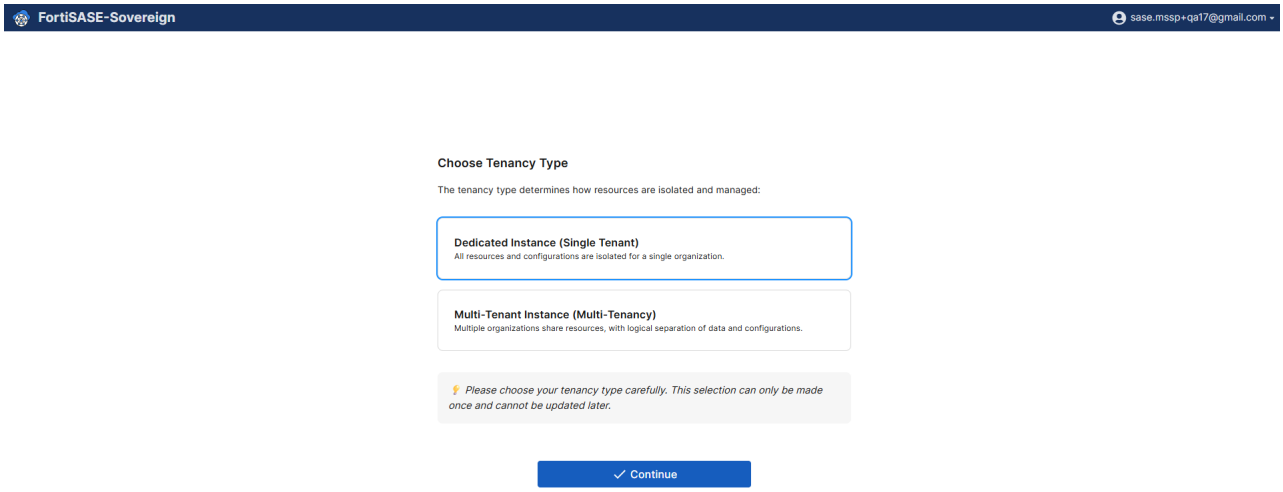
1. Log in using MSSP(root) administrator account.



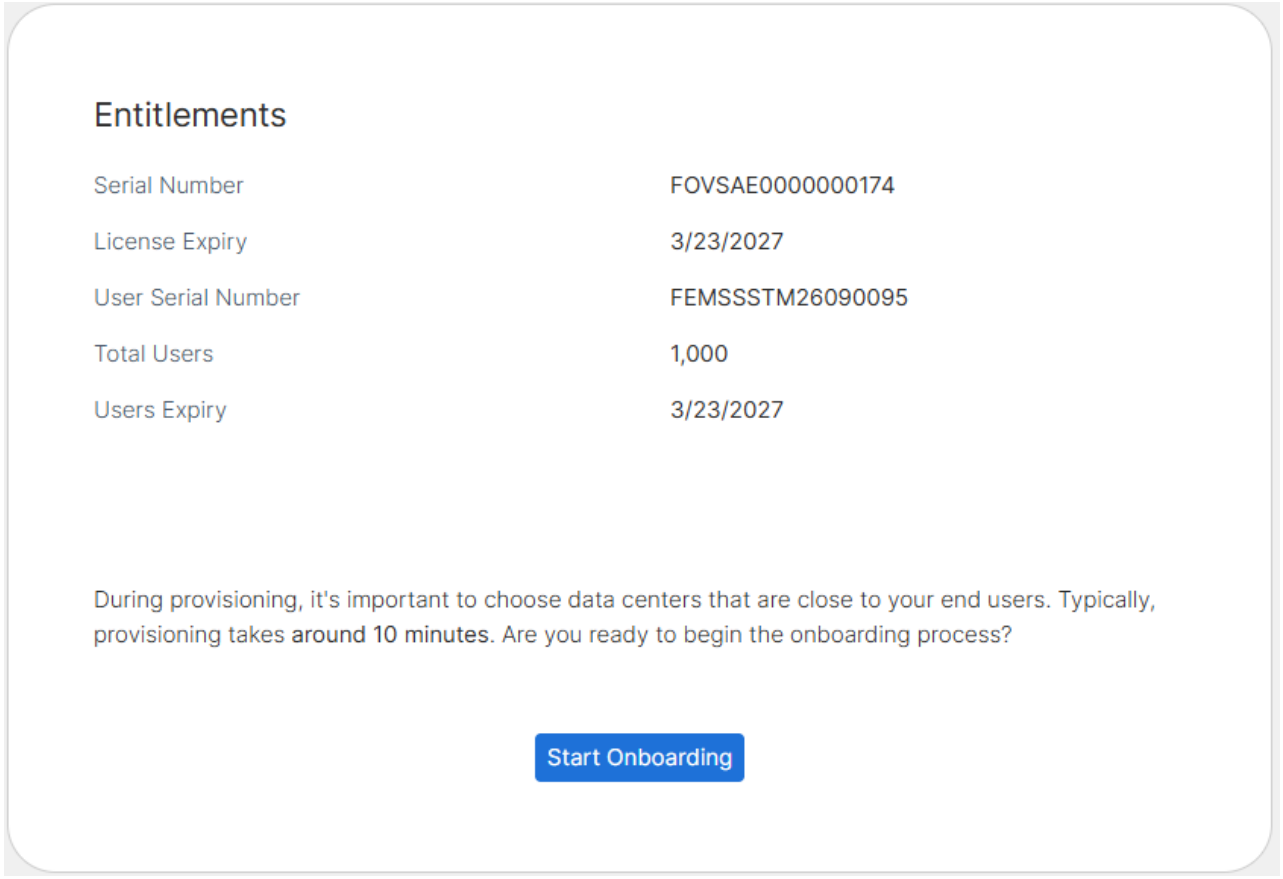
2. Select the region based on your deployment location and compliance requirements, then click Submit.



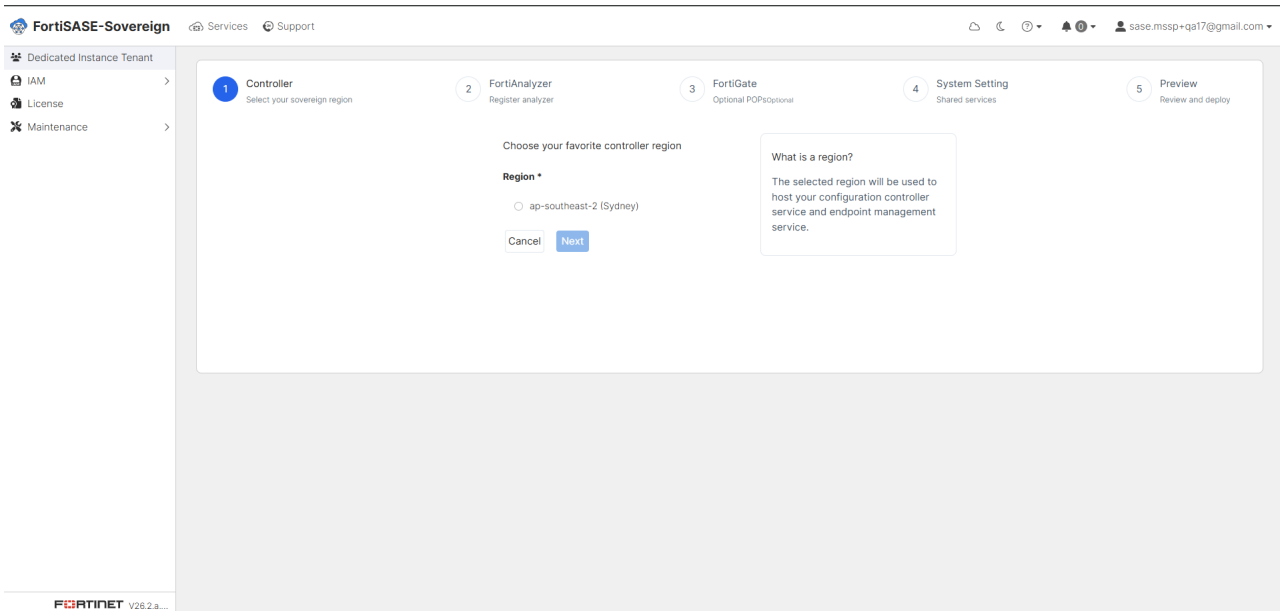
3. select Dedicated Instance (Single Tenant), and click Continue.



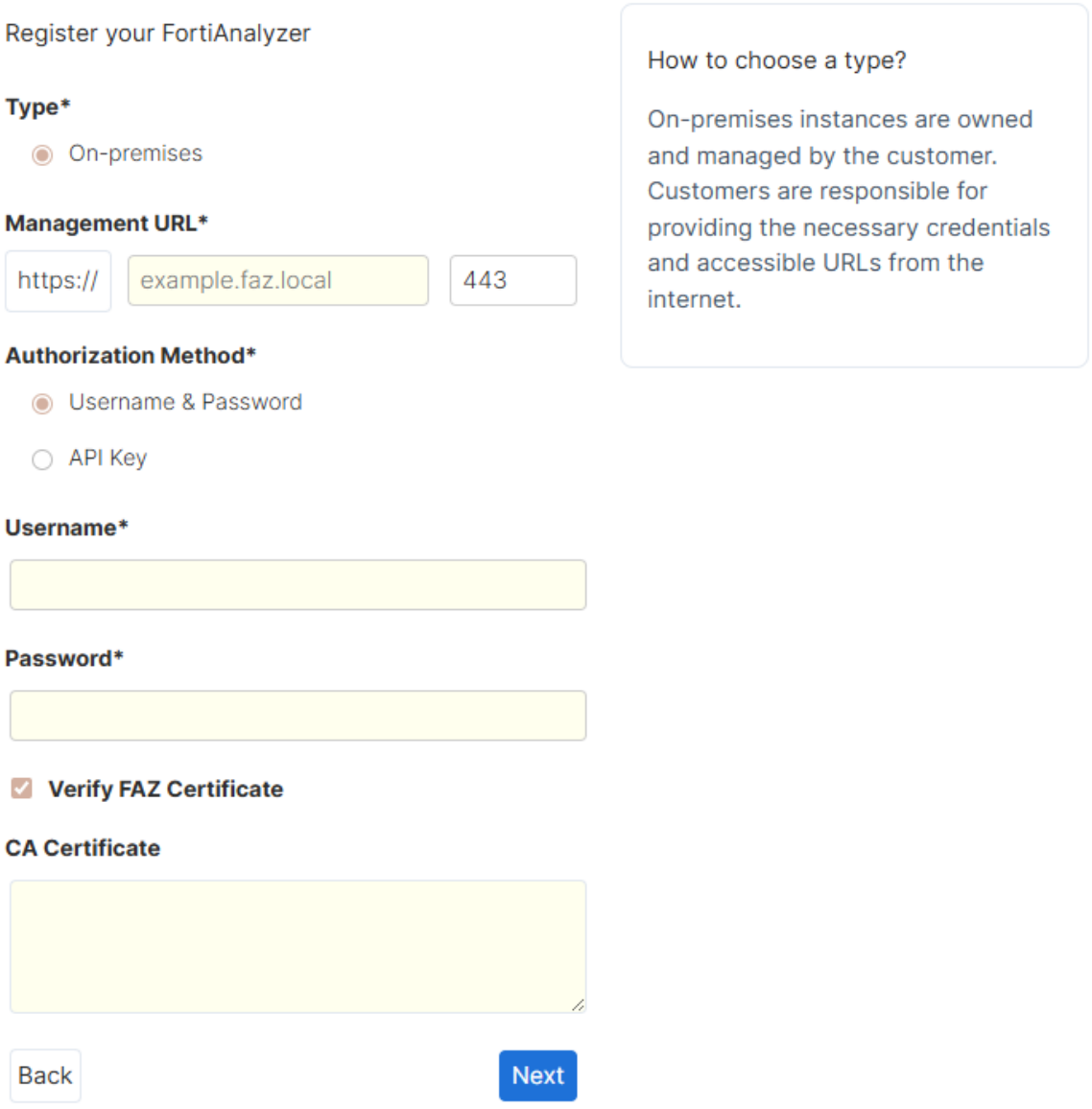
4. Click Start Onboarding to begin the onboarding process.



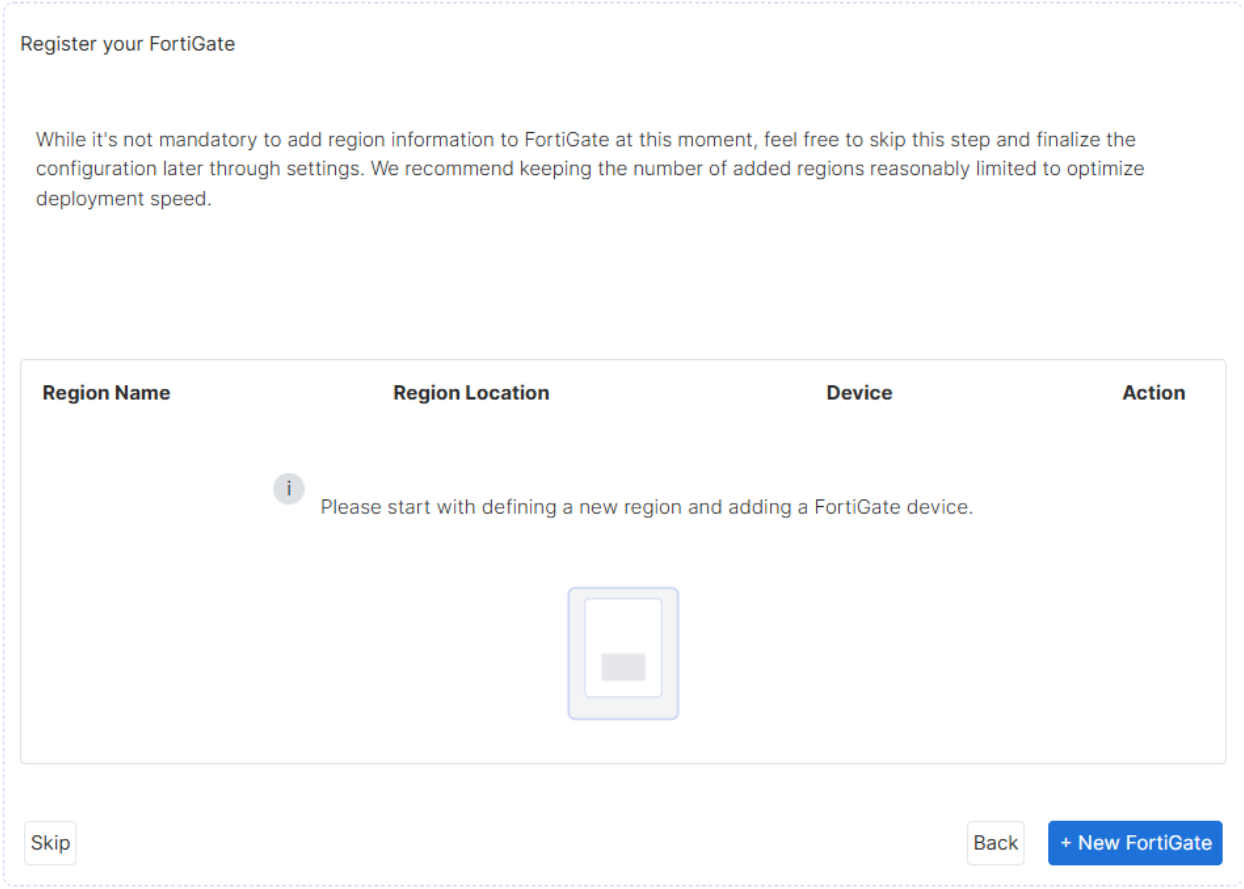
5. Select the deployment region, then click Next.


FortiSASE-Sovereign
Services
Support
sase.mssp+qa17@gmail.com
Dedicated Instance Tenant
IAM
License
Maintenance
1 Controller
Select your sovereign region
2 FortiAnalyzer
Register analyzer
3 FortiGate
Optional POPsOptional
4 System Setting
Shared services
5 Preview
Review and deploy
Choose your favorite controller region
Region *
ap-southeast-2 (Sydney)
Cancel
Next
What is a region?
The selected region will be used to host your configuration controller service and endpoint management service.
FORTINET V26.2.a....

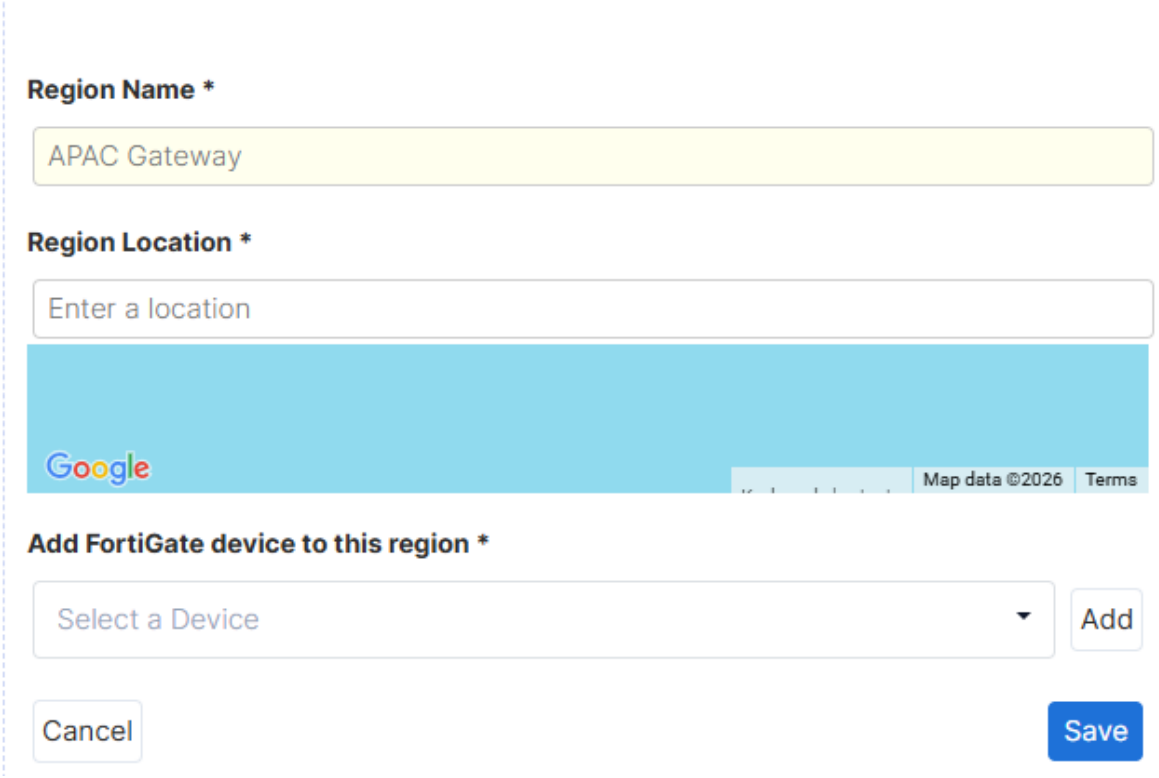
6. FAZ Setup.



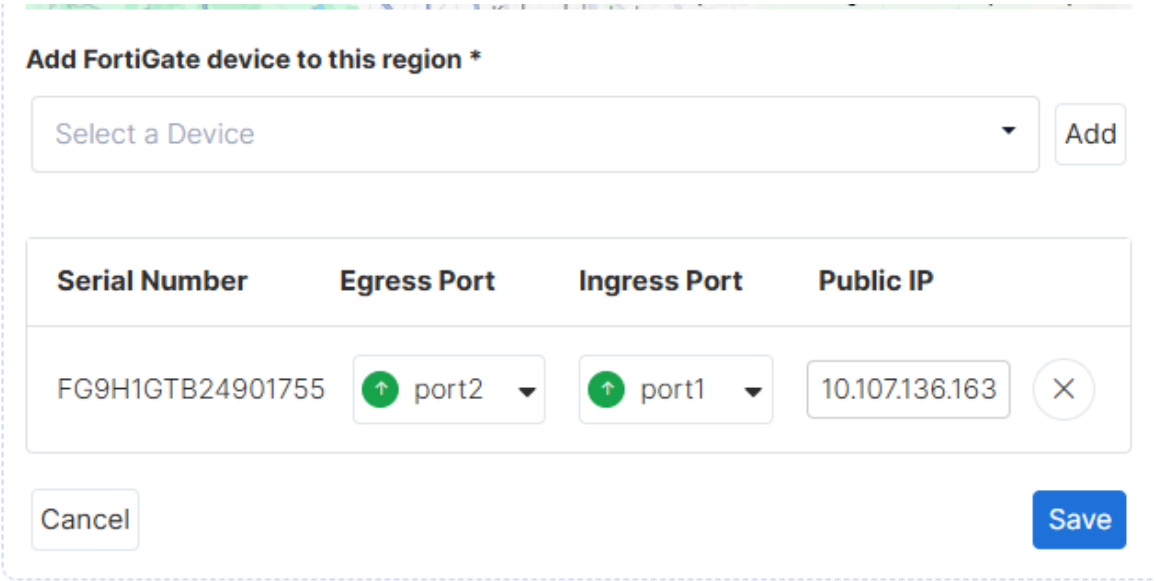
   a. Enter the Management URL (IP address or domain name).
   b. Enter the administrator credentials.
   c. If certificate verification is required, paste the CA certificate content.
   d. Click Next.
7. Add FortiGate.


Register your FortiGate
While it's not mandatory to add region information to FortiGate at this moment, feel free to skip this step and finalize the configuration later through settings. We recommend keeping the number of added regions reasonably limited to optimize deployment speed.
Region Name
Region Location
Device
Action
Please start with defining a new region and adding a FortiGate device.
Skip
Back
+ New FortiGate

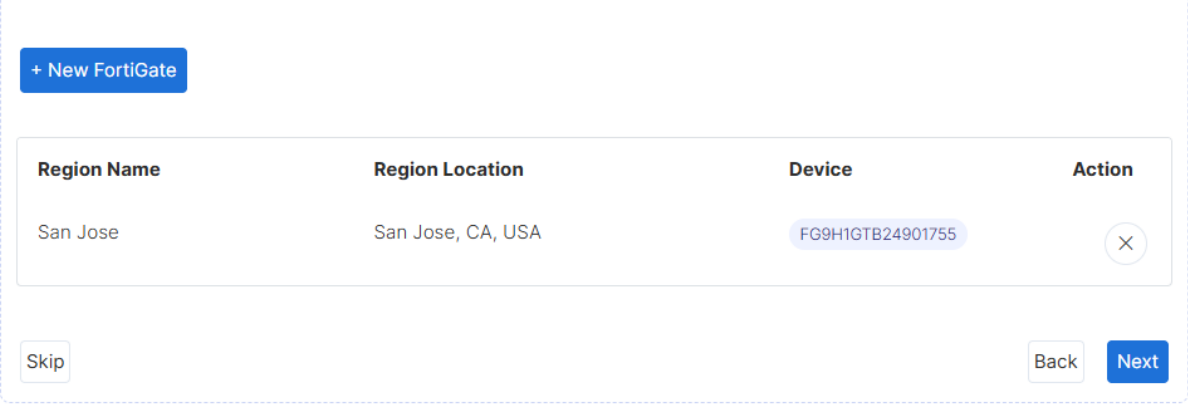
a. Click + New FortiGate to add a device.



b. Select the region name and deployment location.
c. Select an available FortiGate from the Select a Device drop-down list.
d. Click Add.

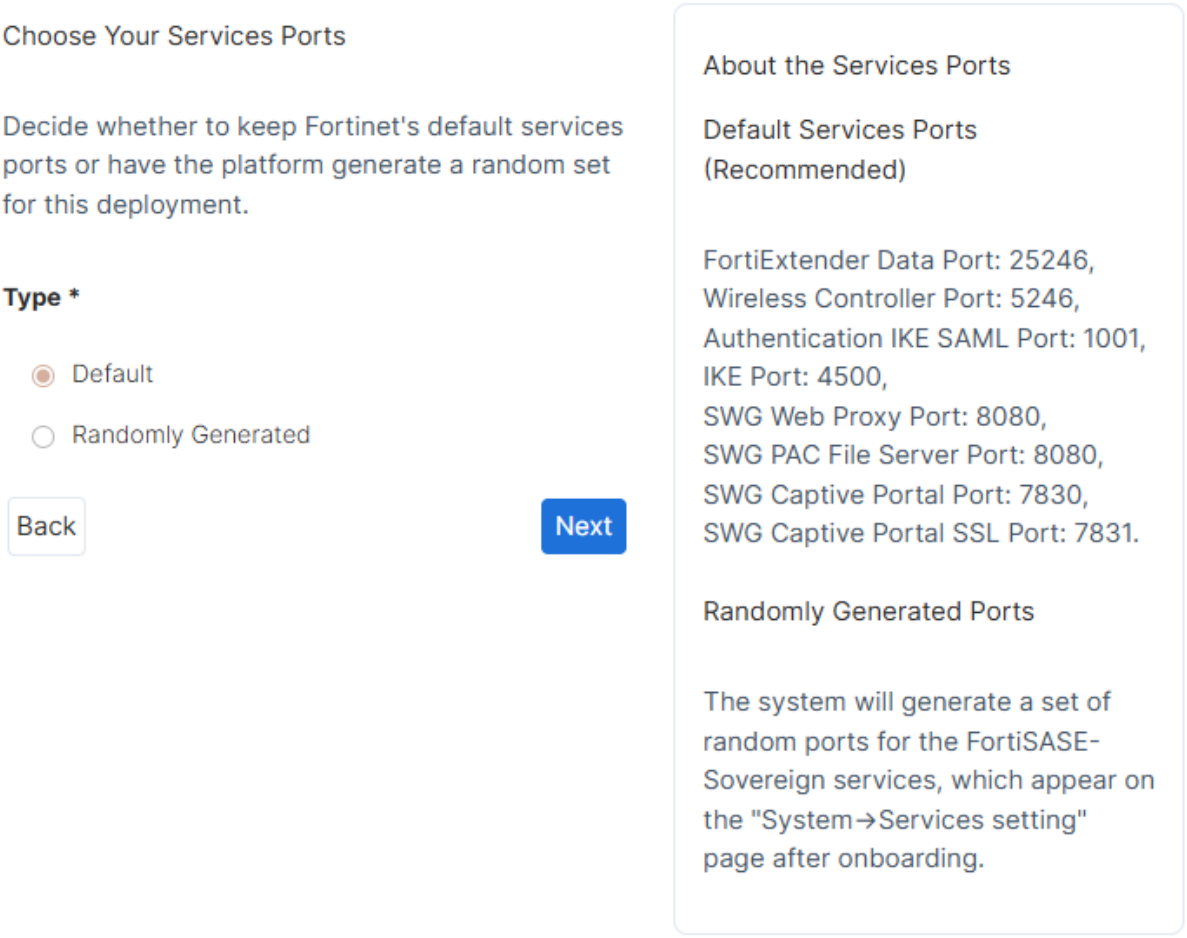


e. Click Save.
f. Repeat this step to add additional FortiGate devices as needed.

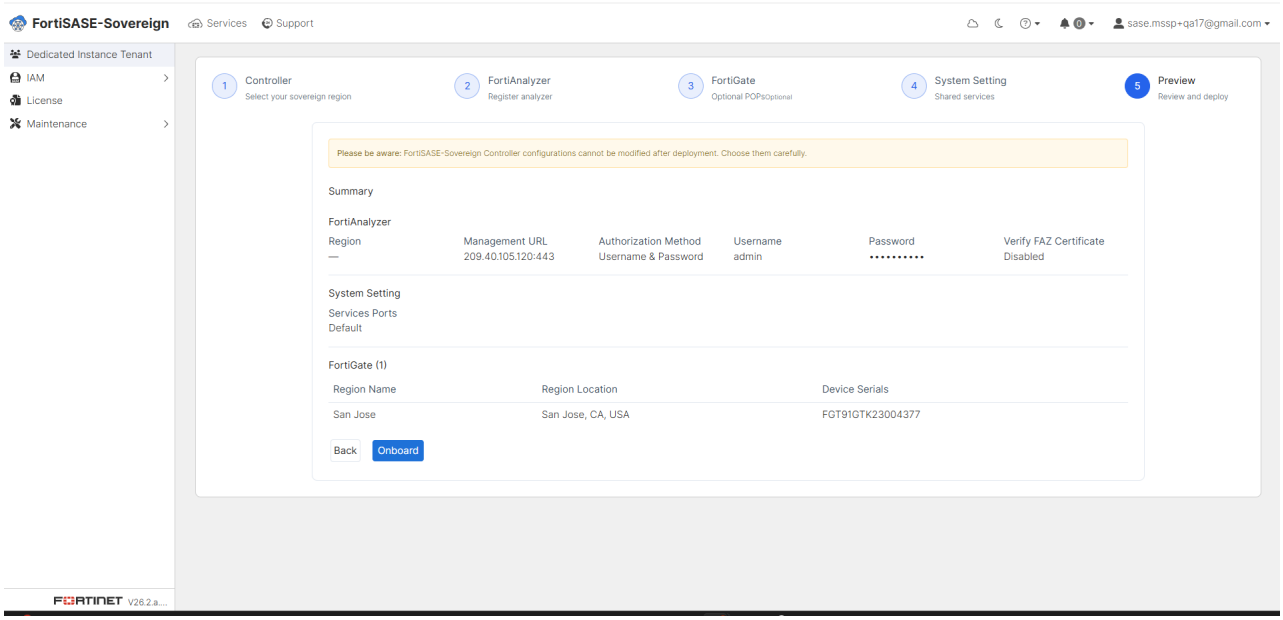


g. After adding all required FortiGate devices, click Next.

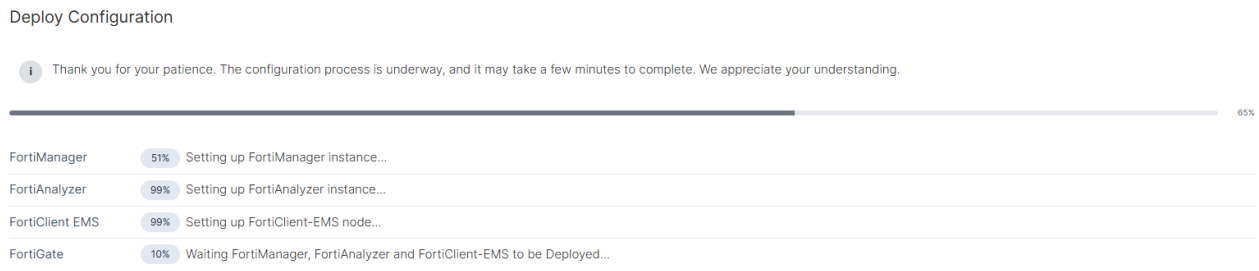
8. Select the required service ports.



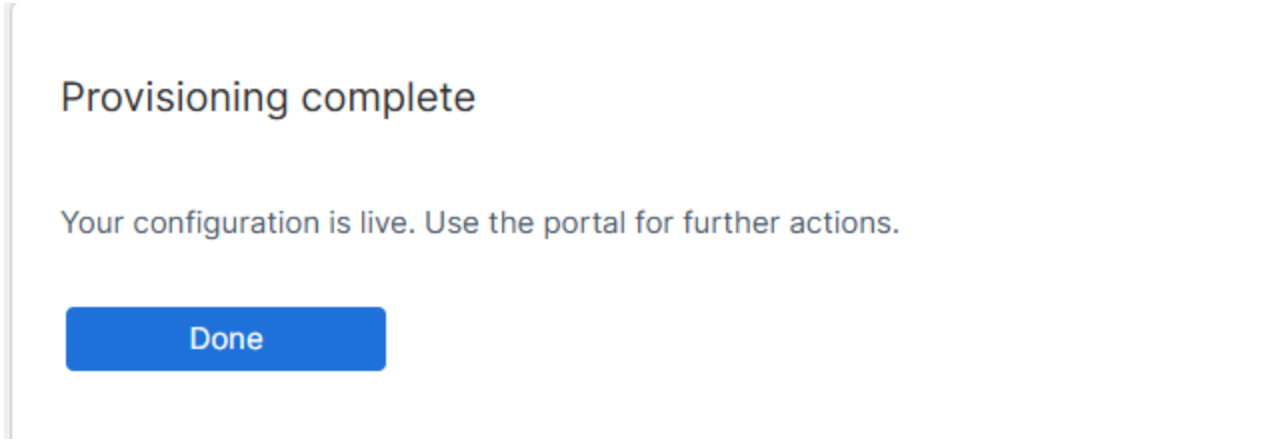
9. Review the configuration summary.



10. Click Onboard to proceed. To make changes, click Back.
11. The system will begin deploying FortiManager, EMS, FortiAnalyzer, and FortiGate services.



12. Onboarding is complete when all components are successfully deployed.

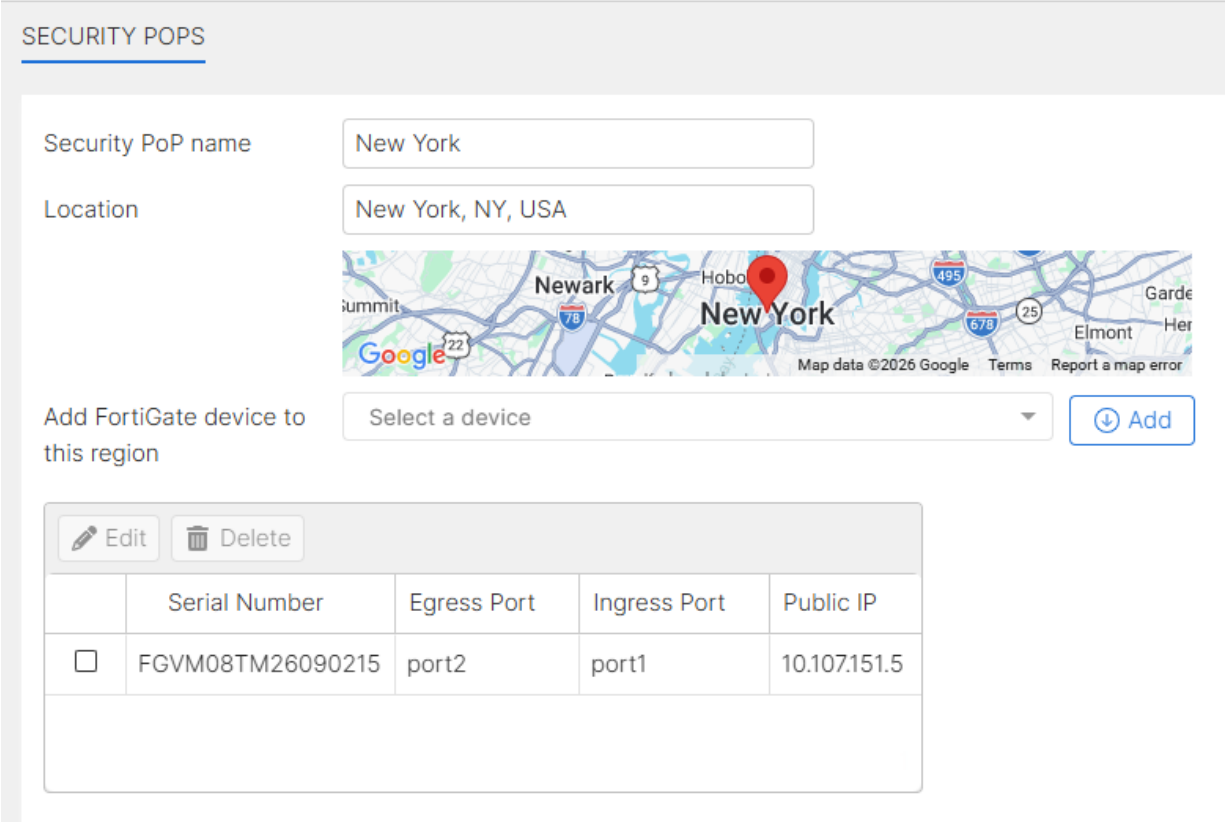


- Note: To verify successful onboarding, go to Device > Security PoPs and confirm that all FortiGate devices are deployed without errors.

Add/Edit/Delete the Security PoPs/FGT

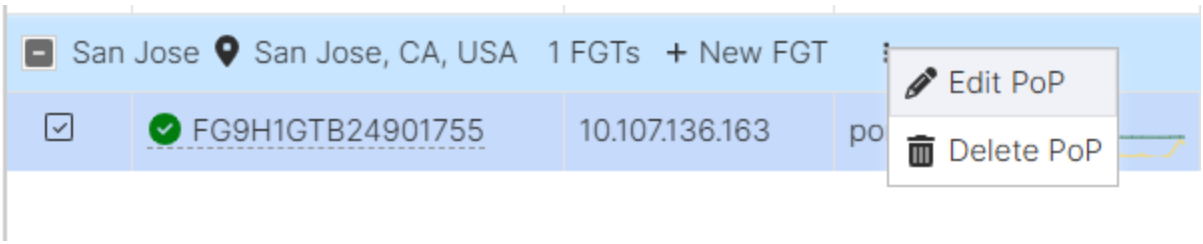
1. Add Security PoP/FGT.
   a. Click “New Security PoP”.

   b. Enter the Security PoP name and location, then add a FortiGate device.

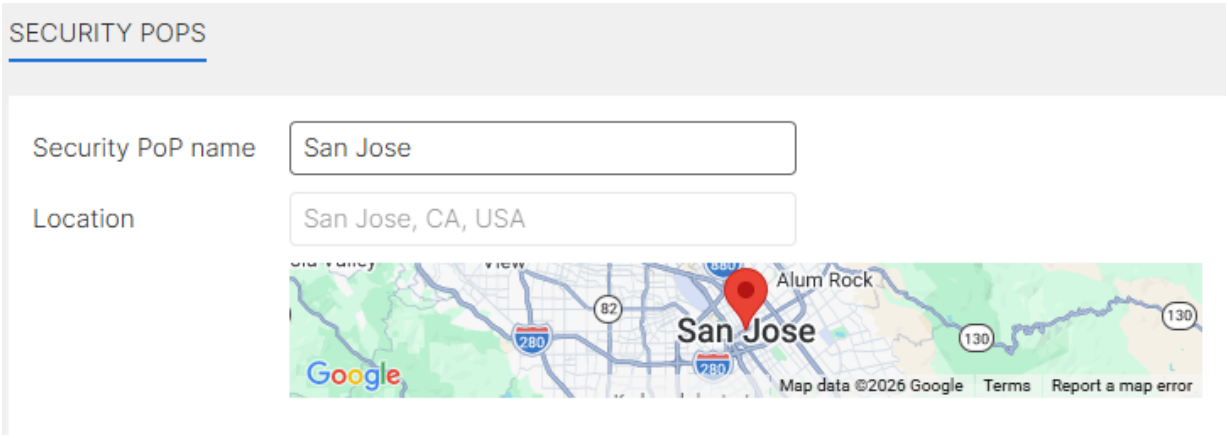


   c. Click “OK”.
   The FortiGate device deployment starts automatically

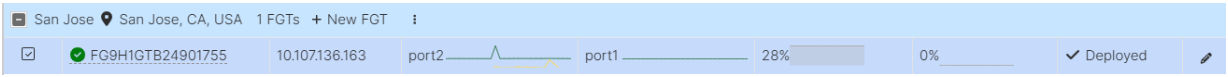
2. Edit Security PoP.



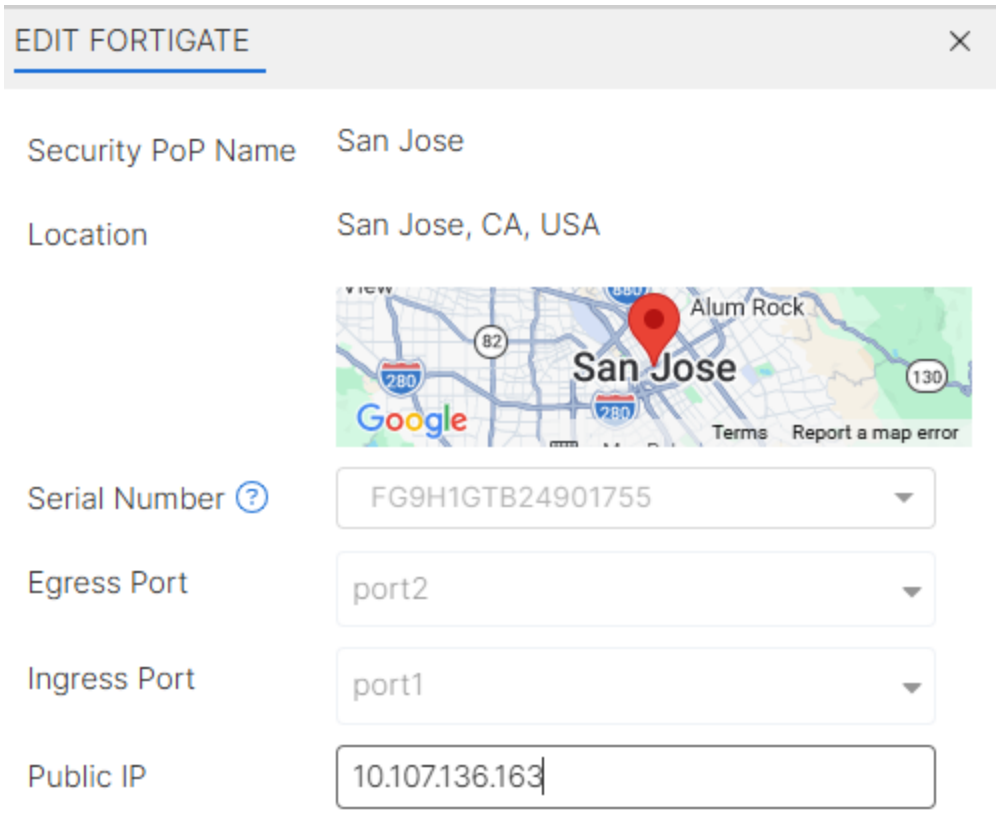
- Only the Security PoP name can be modified.



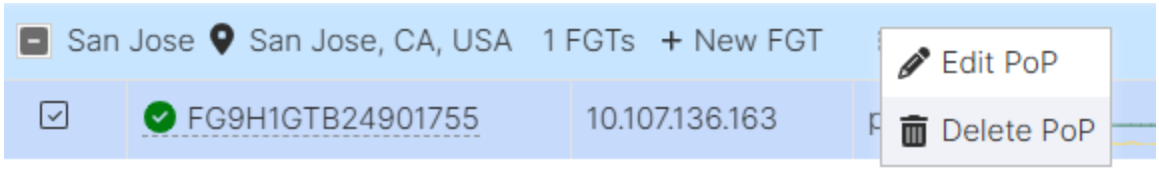
3. Edit FGT.
   a. Click the edit icon next to the entry to modify the FortiGate configuration.



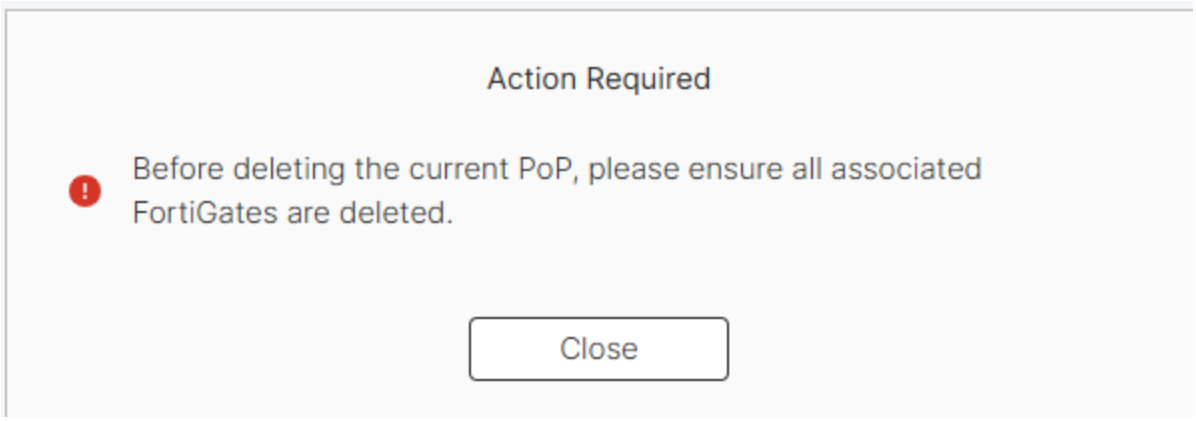
   b. Only the public IP address can be updated.



4. Delete PoP.

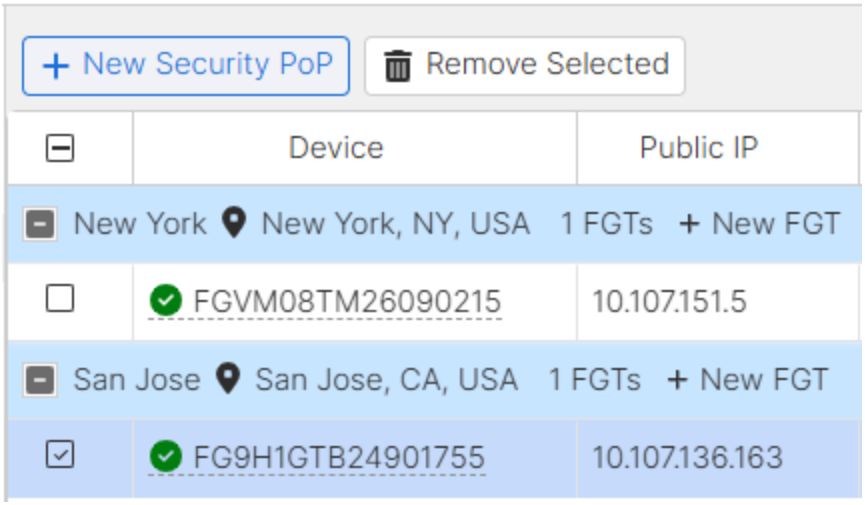


- Remove all FortiGate devices in the Security PoP before deleting the PoP.

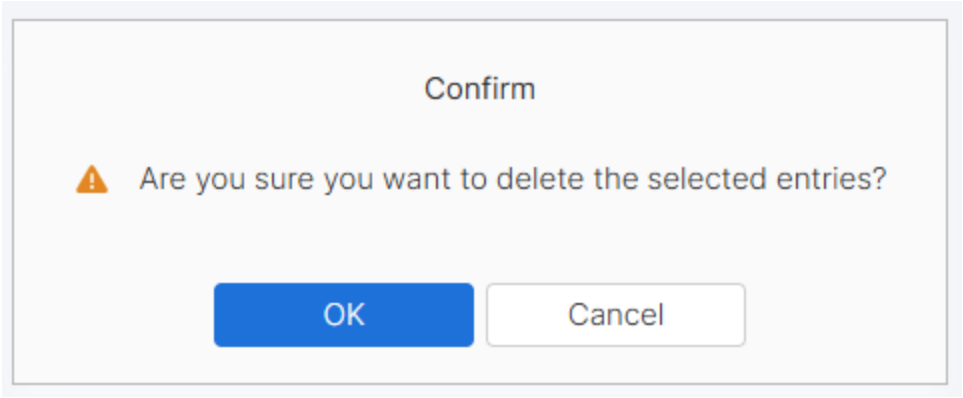


5. Delete FGT.

a. Select a FortiGate device, then click Remove Selected.



b. After confirmation, the selected FortiGate devices will be removed from the deployment.



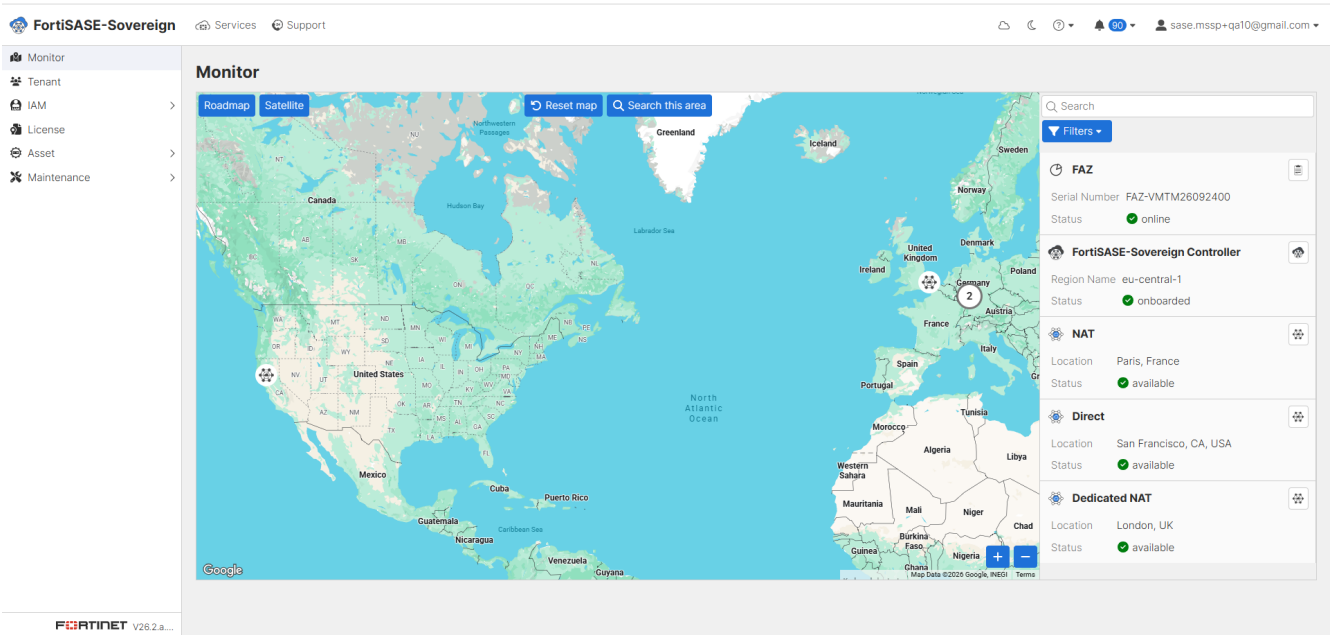
MSSP Protal

Monitor

On the Monitor page, an asset map is available which displays the geographical locations of these FortiSASE Sovereign Controller,FortiAnalyzer and PoPs:

- FortiSASE Sovereign Controller
- Security PoPs
- FortiAnalyzer

You can filter the map using these options.



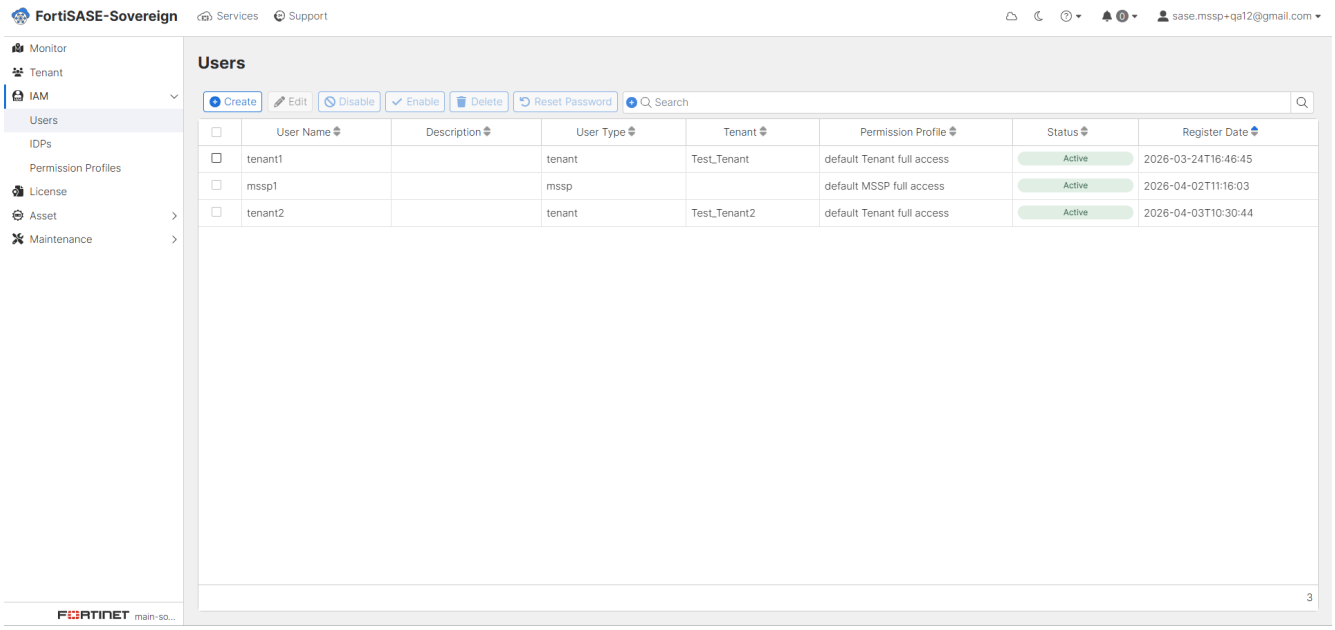
This map helps visualize relative distances between each instance. Also, the map can be helpful with selecting PoPs closest to the location of your agents and edge endpoints.

IAM

Users

The IAM user details can be found in the IAM - User page, including User name, Description, User Type, Tenant, Permission Profile, Status and register date. Use this page to add and delete users, or temporarily disable a

user. Click Create to add a new IAM User. Click the user's User Name to edit their profile, update their permission profile. Click “reset password”reset their password. After the user is created, you can update the user's permission profile at any time from the User Permission tab.



Create IAM users

To create an IAM user:

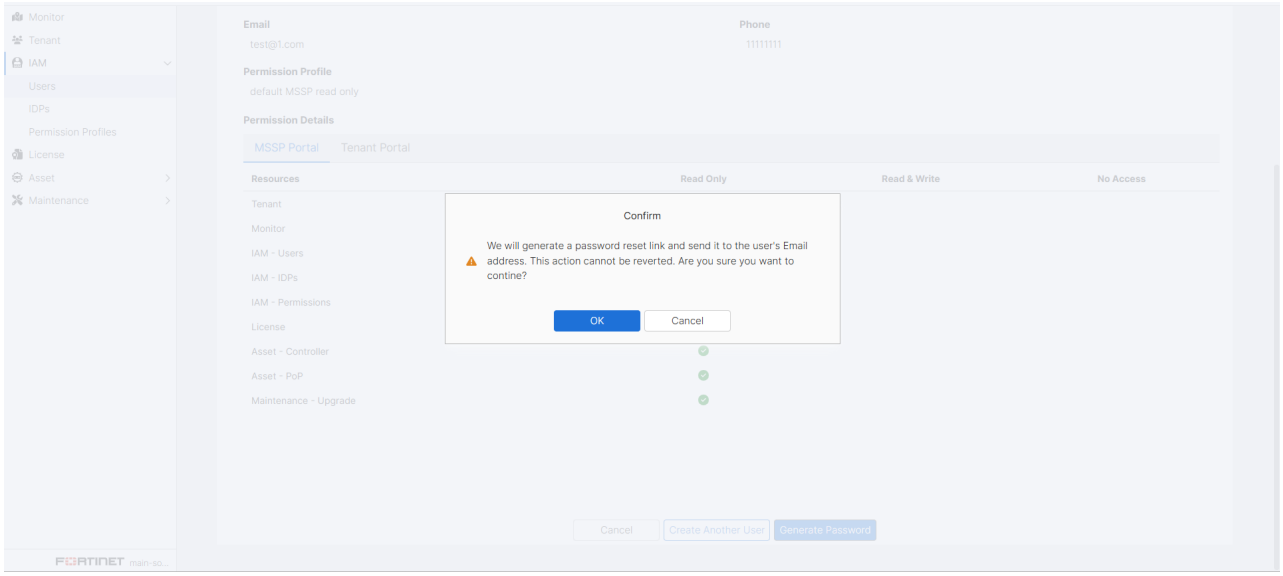
1. Select Users from the left-hand navigation menu. The Users page opens.
2. Click Create. The Create User pane opens.
3. Enter the user's details and click Next.

Account Info	Description
Username	Type the username with no spaces.
Full Name	Type the user's name.
Email	Type the user's email address.
Phone	Type the user's phone number.
Description (Optional)	Type a description of the user.

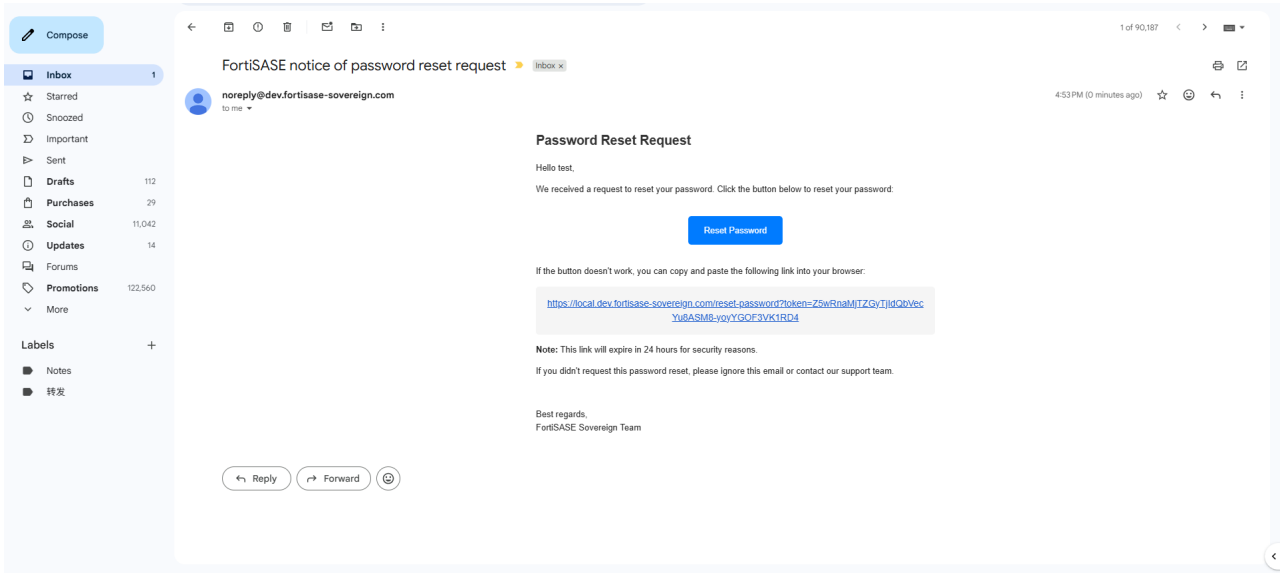
4. Select a Permission Profile and click confirm.
5. Click “Generate Password” to reset password.

Generating the password reset:

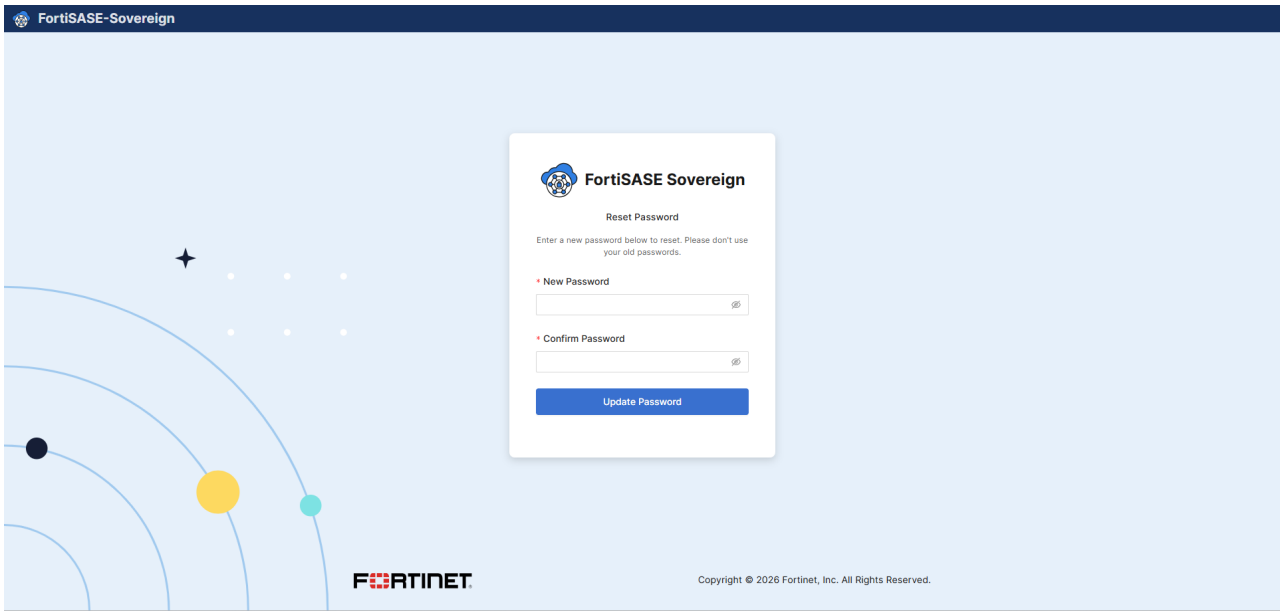
1. After create user, click “Generate Password”.
2. Popup a notification, click “Confirm”.



3. After received reset email, click “Reset password” link.



4. Enter the password in the New Password and Confirm New Password fields.



Login as IAM Users:

Users can access FortiSASE Sovereign services and support as an IAM user with their IAM user credentials.

While it is optional, all new IAM Users will auto enable Two-Factor Authentication (2FA).

To log in as an IAM user:

1. Click FortiSASE Sovereign invitation email link.
2. Input Account ID which you can get from previous email.
3. Input IAM - Username and click Login.
4. Input credential and click Login.

IDP

FortiSASE Sovereign supports using an external identity provider with SAML 2.0 authentication. Once the setup is complete, external users can authenticate with the desired provider and access FortiSASE Sovereign services based on the roles defined by the administrator.

FortiSASE Sovereign supports fine grained permission profiles for external IdP users through IAM Permission Profile. External IdP roles are authenticated with a custom login page. After the user is authenticated, they are redirected to a page where the administrator assigned to their account.

Note: IDP will only be available in Multi Tenancy mode.

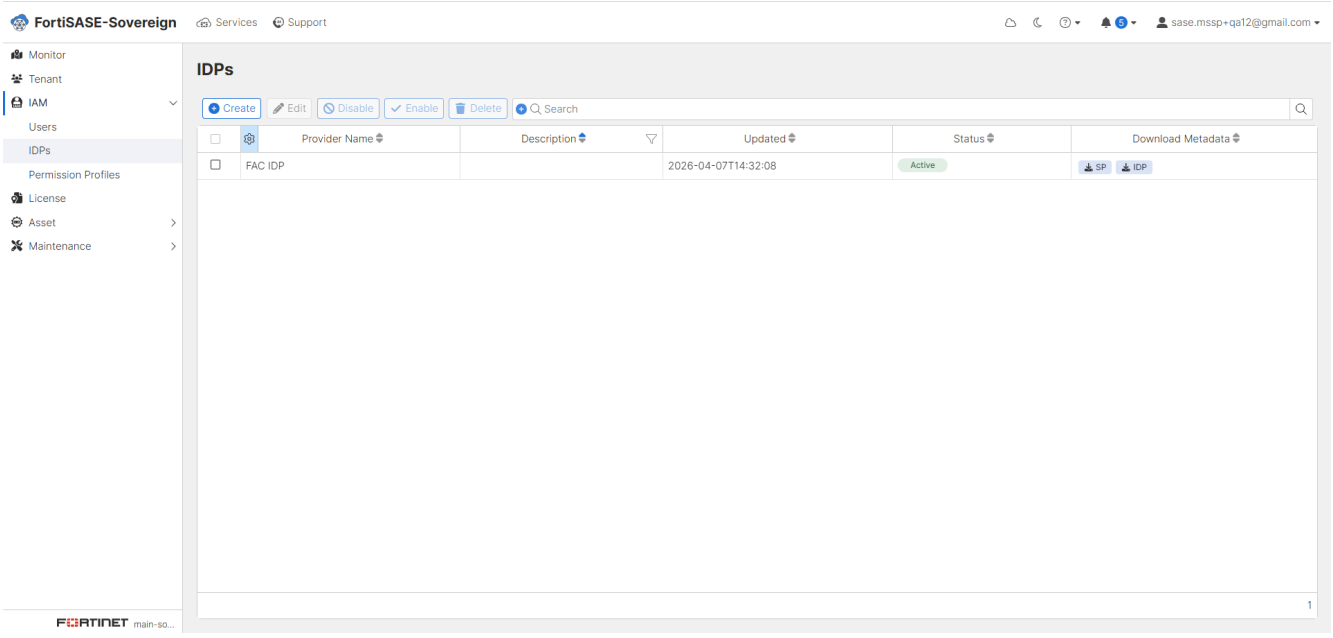
Configuring IDP Server

To Configuring an IDP Server:

1. Click Create to add a new IDP Server.
2. Enter the IDP Server details and click Confirm.

Configuration Settings	Description
Name	Type the server name.
Upload IDP Metadata	Import IDP Metadata profile.
Domains	Type the domains to be used for IAM User access.
Username Attribute	Enter the value as set in your IdP configuration.
Tenant ID Attribute	Enter the value as set in your IdP configuration.
Permission Profile Attribute	Enter the value as set in your IdP configuration.
Select Tenant	Enter the value as set in your IdP configuration. If set, this value is used to match the tenant user with an onboarded tenant.
Select Permission Profiles	This value is used to match the Permission Profile assigned by administrator.
Description	Type a description of the IDP Server.

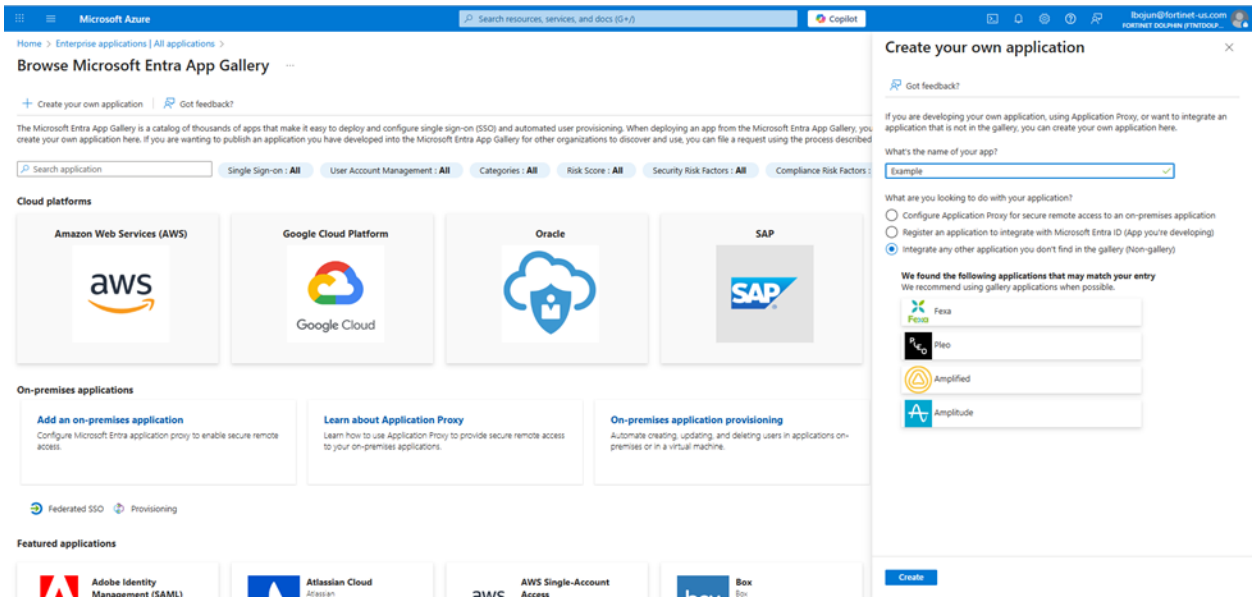
3. Download the SP Metadata under “Download Metadata” column and import back to IDP Server.



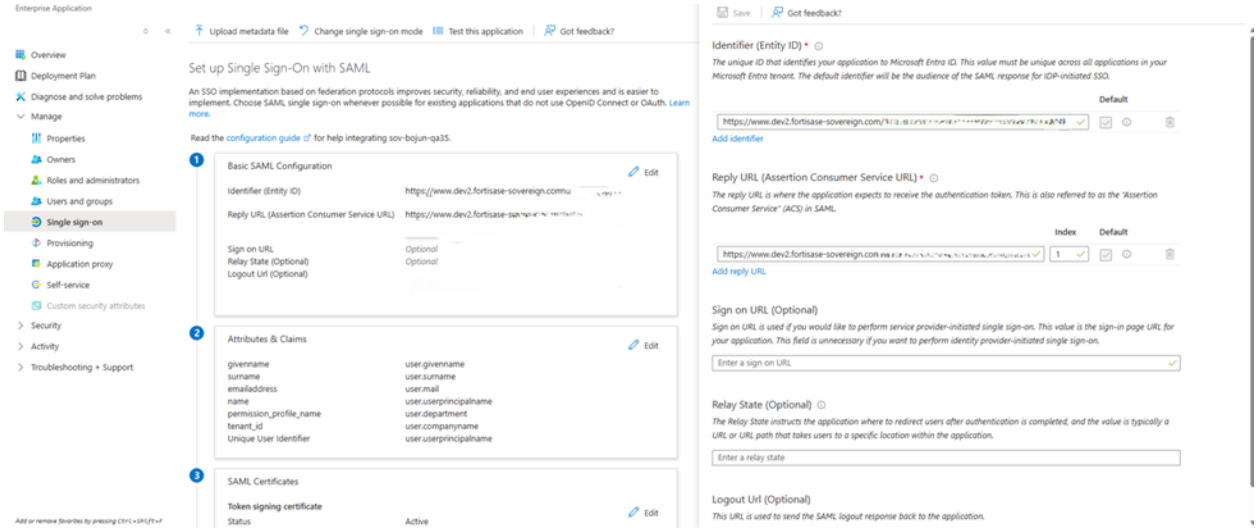
Example of configuring Azure IDP:

To add an Azure IDP server:

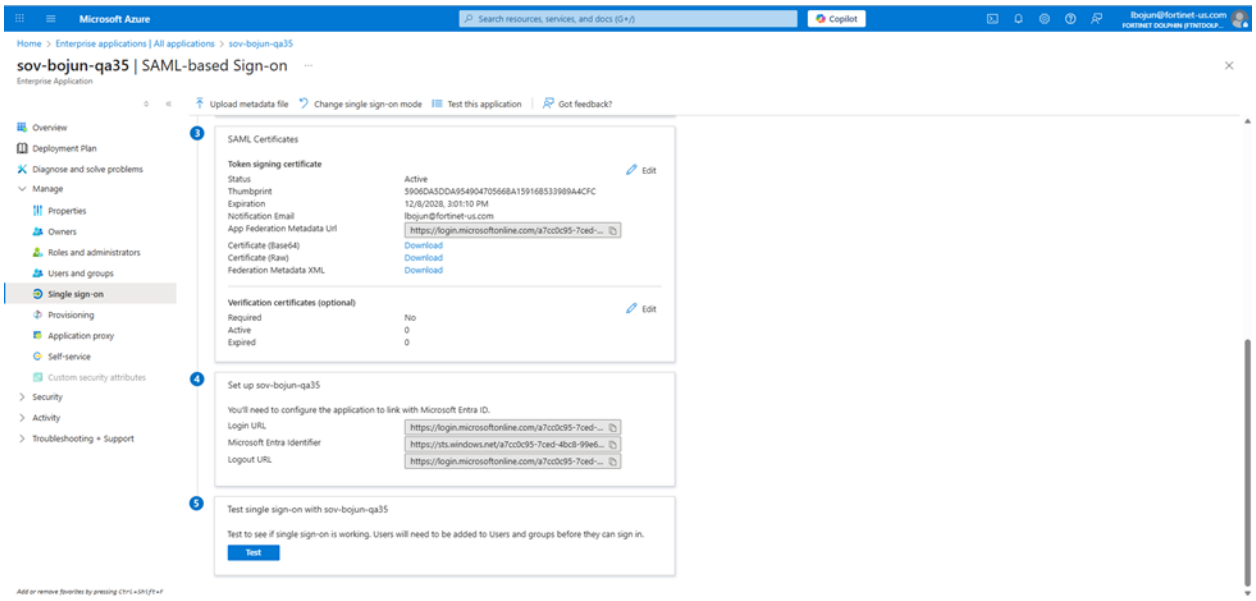
1. Create an new application on Azure.



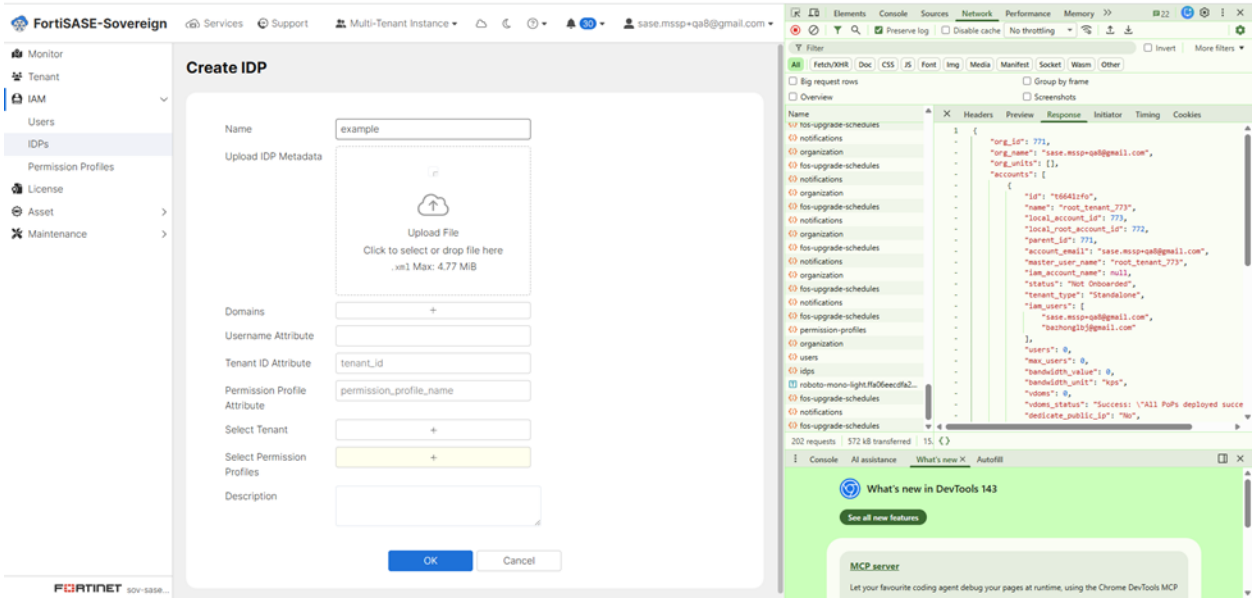
2. Go to SAML Configuration.
3. Input some fake data into “Entity ID” and “ACS URL”(We will update real data here later).



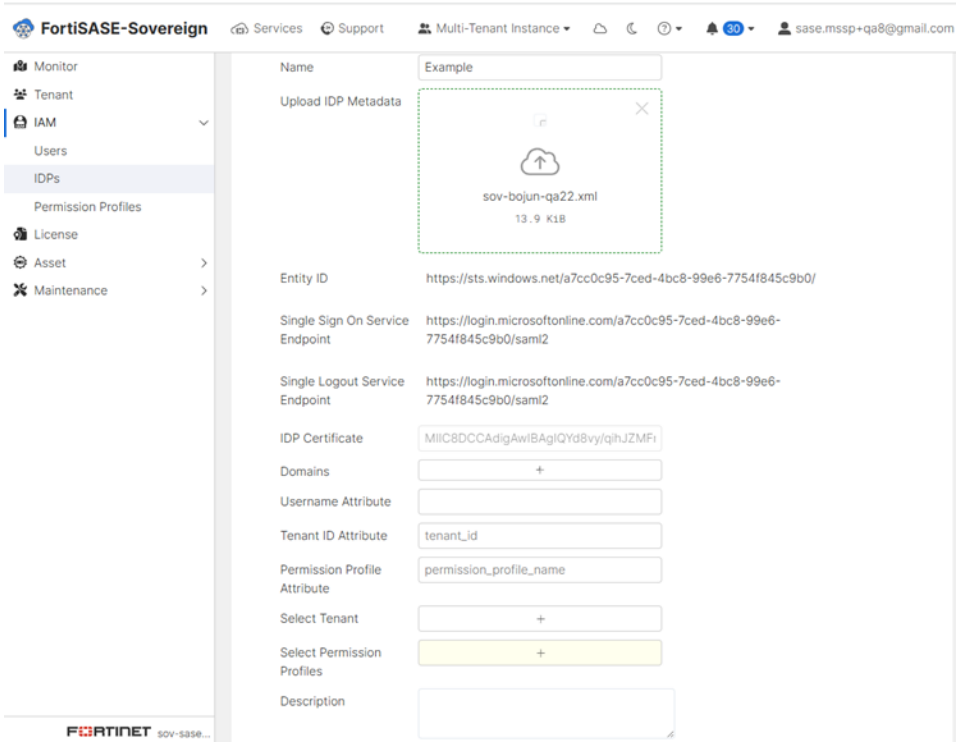
4. Download IDP Metadata from SAML Certificates - Federation Metadata XML.



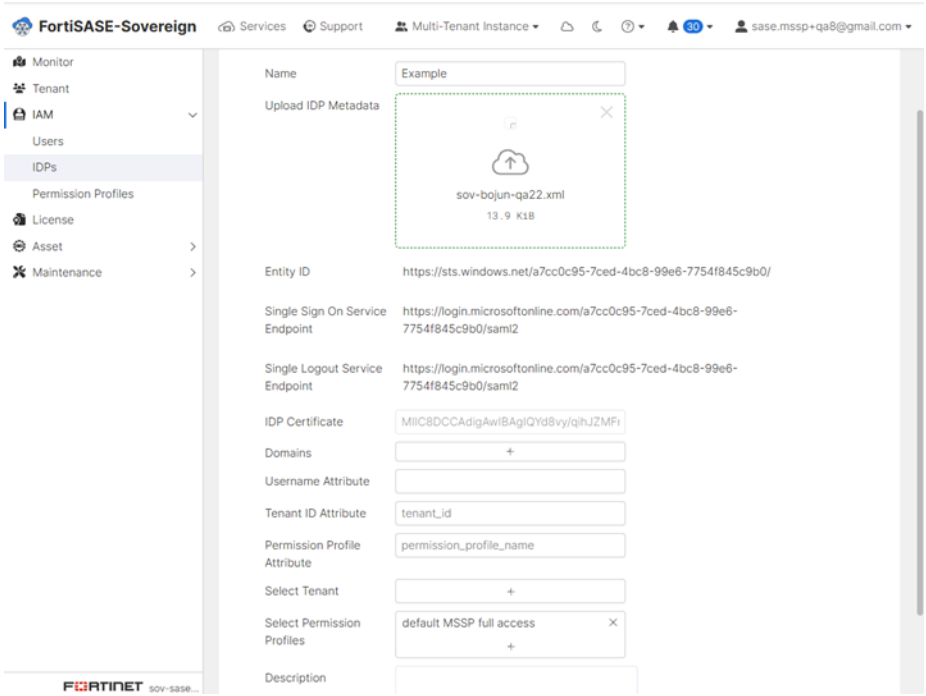
5. Go to MSSP Portal and create new IDP(Default username always read “Unique User Identifier (Name ID)” when it’s empty here).



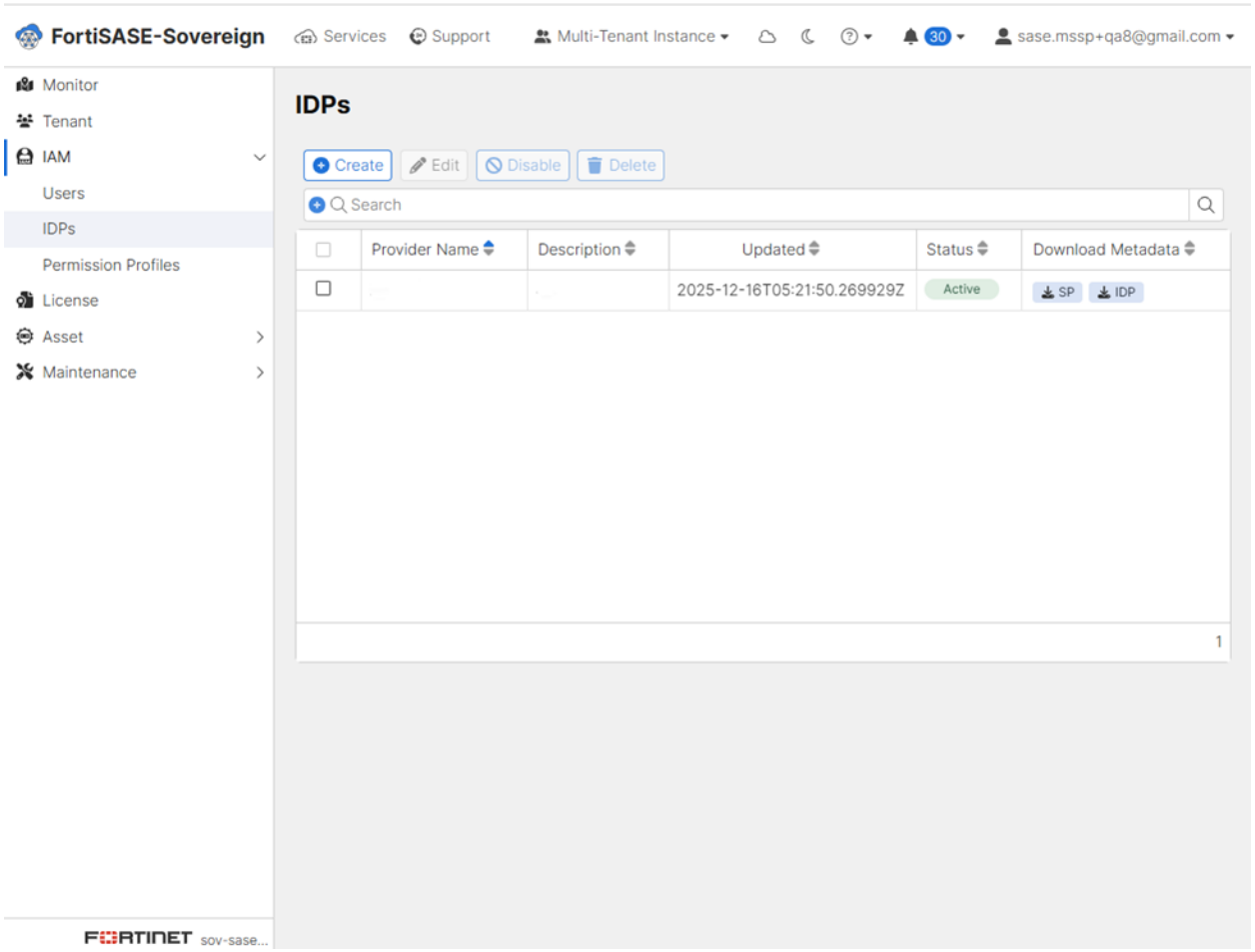
6. Upload your downloaded Metadata file.



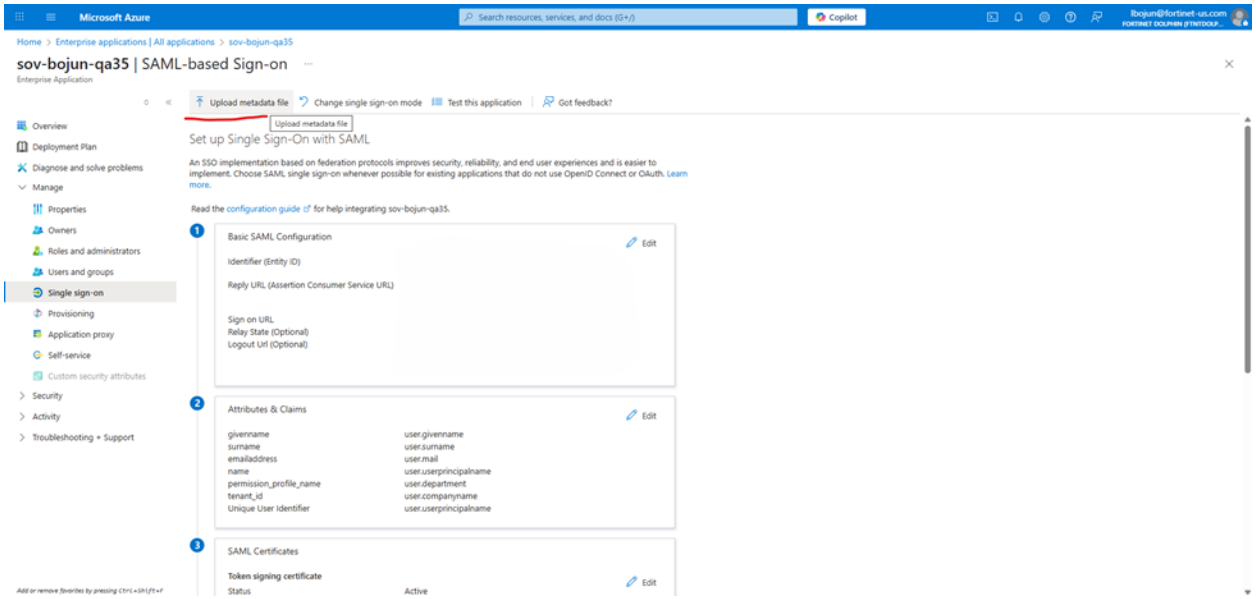
7. Config “Select Permission Profile”(If you select any Tenant Permission Profile, you must also choose “Select Tenant” to add Tenant ID).



8. Click save and Download “SP” from “Download Metadata”.



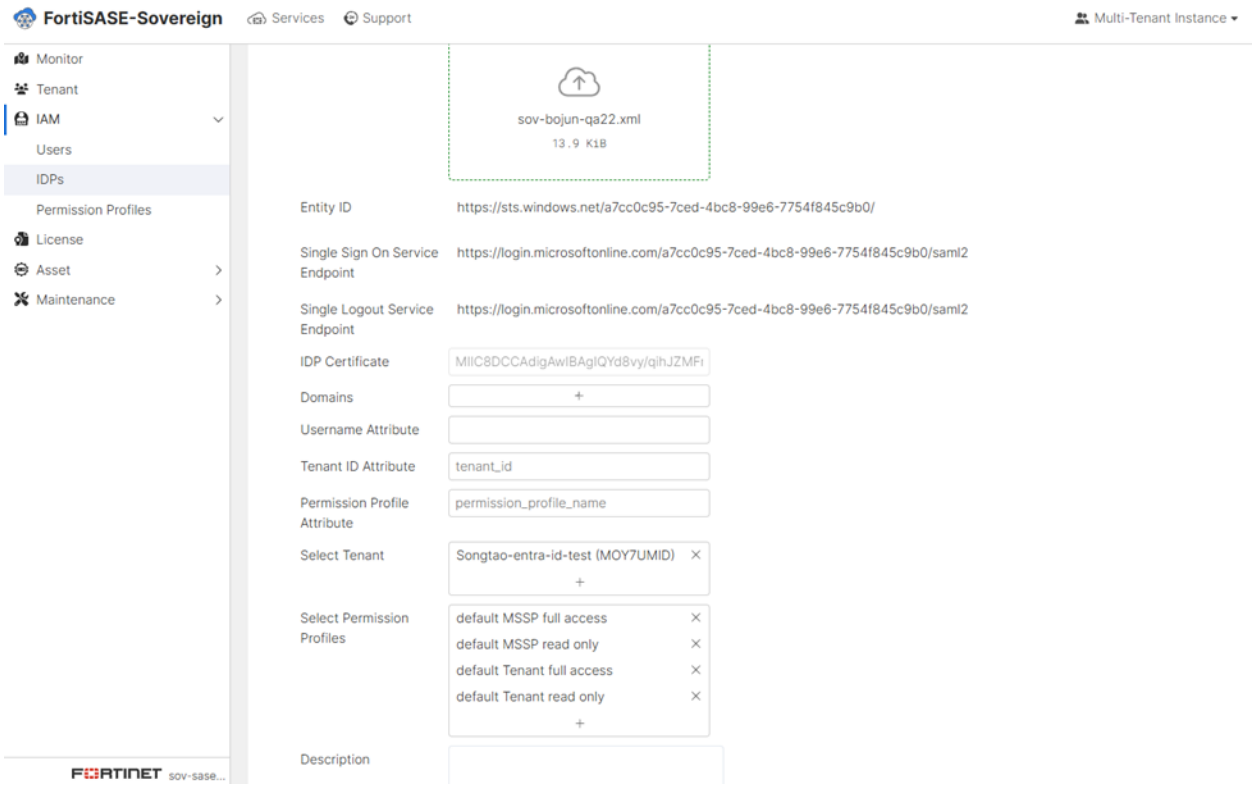
9. Upload SP File back to Azure.

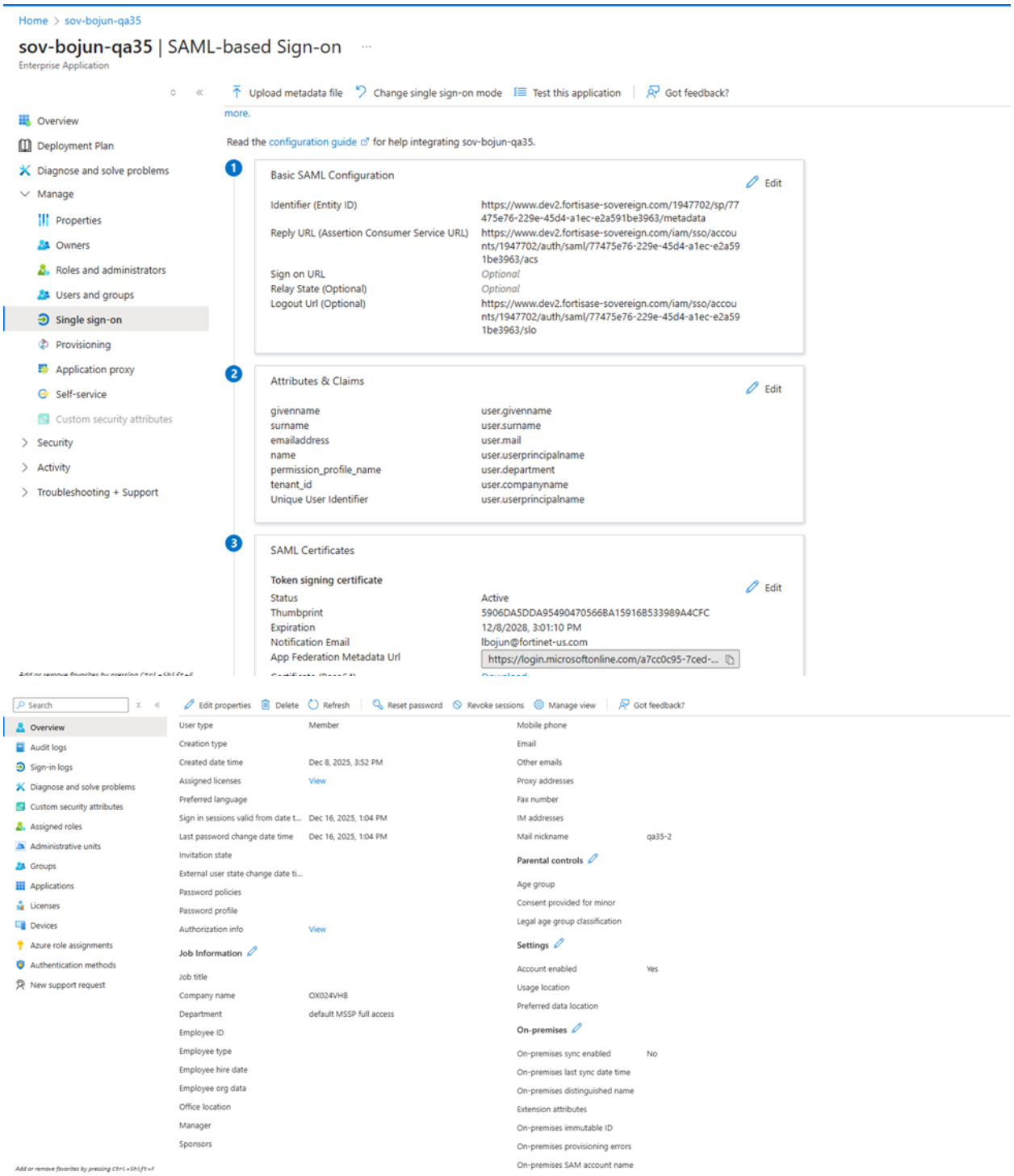


10. Config SP Attribute to IDP(Create new Claim in Azure, name should as same as value in Username/Tenant ID/Permission Profile attribute name).

Base on below config in “IDP”, we should add following new claim to Azure.
“tenant_id”: “user.companyname”
“permission_profile_name”: “user.department”
For IDP users, we need to add following config to match SP settings:
MSSP User:
Company:
(We can leave it empty here because MSSP User don’t need specific tenant ID)
Department: default MSSP full access

Tenant User:
Company: MOY7UMID
Department: default Tenant full access





Permission Profiles

Permission profiles define the level of portal access and permissions a user has. Permission profiles allow you to access portal-specific permissions for the enabled portals.

Permissions will be role-based on the portal:

Role-based permissions can be read-only, read and write, or no-access levels with more specific permissions available depending on the different types of portals.

Create Permission Profile

A new permission profile can be made from the Permission Profiles page.

Notes:

In Dedicate mode, will include Admin and Tenant Type permission profile

In Multi mode, will include MSSP and Tenant Type permission profile

Admin Permission will support following permission types:

Permission Category	Type
IAM - Users	• Read Only • Read & Write • No Access
IAM - Permissions	• Read Only • Read & Write • No Access
License	• Read Only • Read & Write • No Access
Maintenance - Upgrade	• Read Only • Read & Write • No Access

Tenant Permission will support following permission types:

Permission Category	Type
Dashboard	• Read Only • Read & Write • No Access
Device	• Read Only • Read & Write • No Access

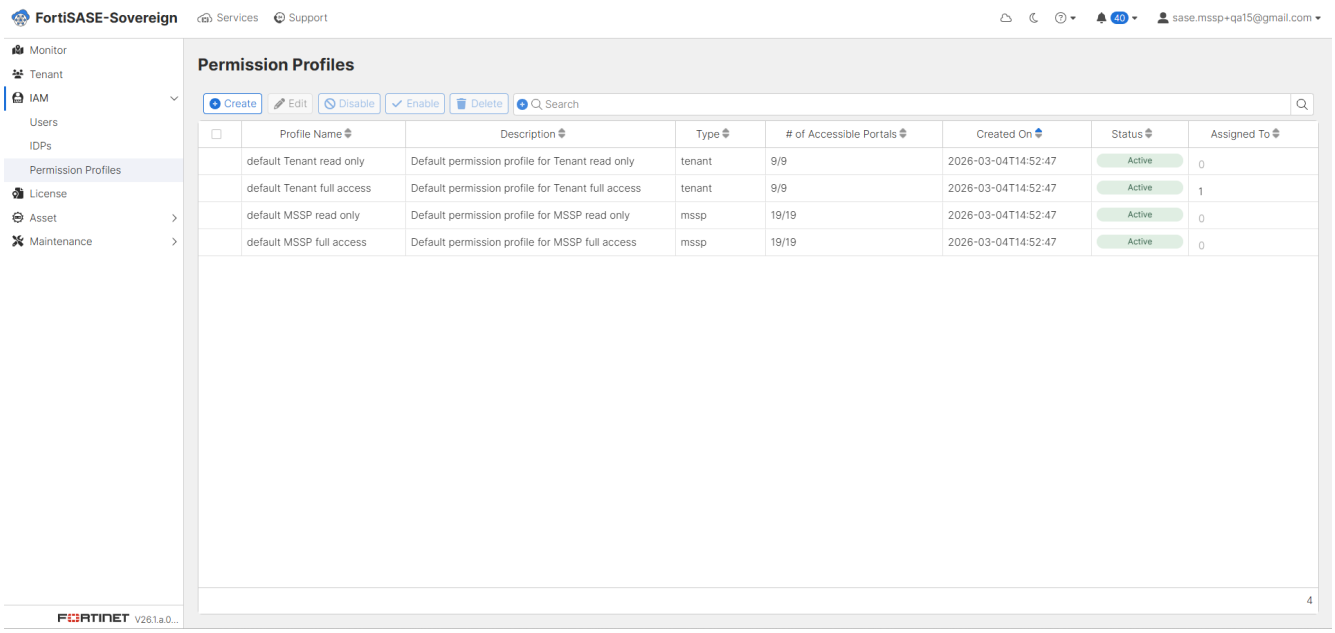
Permission Category	Type
Edge Devices	• Read Only • Read & Write • No Access
Access & Authentication	• Read Only • Read & Write • No Access
Security	• Read Only • Read & Write • No Access
Endpoint Management	• Read Only • Read & Write • No Access
SDWAN	• Read Only • Read & Write • No Access
System	• Read Only • Read & Write • No Access
Analytics	• Read Only • Read & Write • No Access

MSSP Permission will support following permission types:

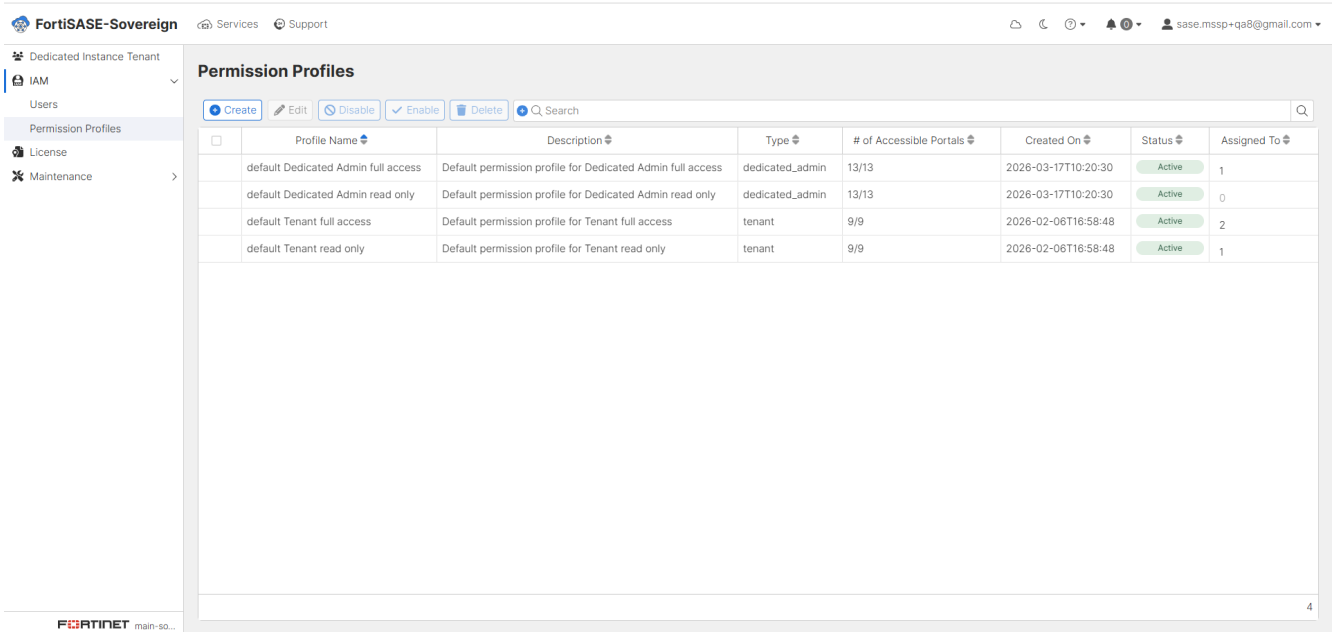
Permission Category	Type
Tenant	• Read Only • Read & Write • No Access
Monitor	• Read Only • Read & Write • No Access
IAM - Users	• Read Only • Read & Write • No Access
IAM - Permissions	• Read Only • Read & Write • No Access
License	• Read Only

Permission Category	Type
	• Read & Write • No Access
Asset - Controller	• Read Only • Read & Write • No Access
Asset - PoP	• Read Only • Read & Write • No Access
Maintenance - Upgrade	• Read Only • Read & Write • No Access

Multi Mode:



Dedicate Mode:



Create a Permission Profile:

1. Go to IAM - Permission Profile pane and click Create.
2. Select desired permission details and click Ok.

Configuration Settings	Description
Permission Profile Name	Type Permission Profile name.
Status	Type desired Status.
Description	Type Permission Profile description.
Type	Select desired Permission Type.

Manage Permission Profile

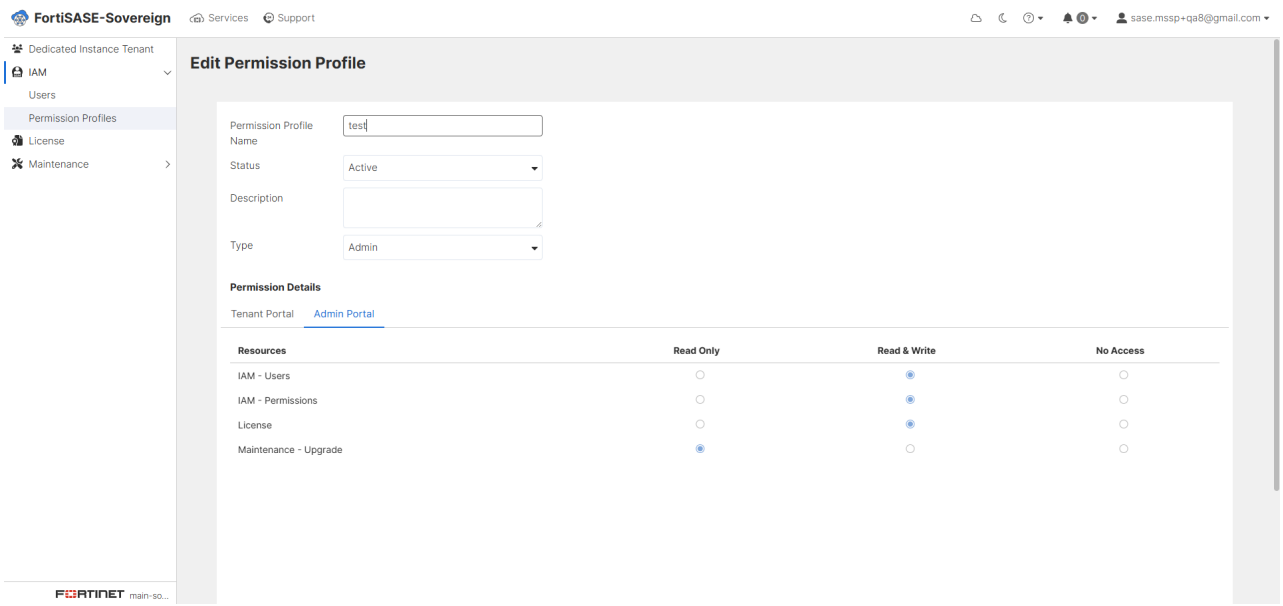
Permission profiles are listed on the Permission Profiles page. By selecting a permission profile, you can edit specific details of the profile.

Note: You cannot edit, disable, or delete the default permission profile

Editing a permission profile

To edit a permission profile:

1. Select Permission Profiles from the left-hand navigation menu.
2. Select the permission profile you want to edit. Click Edit. The details page is displayed.



3. Make changes can be made to all attributes.
4. Click Ok. The profile has been updated for all users assigned to it.

Note: Upon updating the permission profile, all linked IAM users will be required to re-authenticate. Please allow a few minutes for the new permissions to propagate and become active.

Disabling a permission profile

If a permission profile is not needed at the moment, but may be required in the future, it can be temporarily disabled. A permission profile cannot be disabled if an active IAM user is assigned to it.

To disable a permission profile:

1. Select Permission Profiles from the left-hand navigation menu. The Permission Profiles page opens.
2. Select the profile you want to disable.
3. Click Disable. The profile and any assigned users are disabled.

Deleting a permission profile

You can permanently delete a permission profile that is no longer needed. A permission profile cannot be deleted if an active IAM user is assigned to it.

To delete a permission profile:

1. Select Permission Profiles from the left-hand navigation menu. The Permission Profiles page opens.
2. Select the profile you want to delete.
3. Click Delete.

License

The License page provides a centralized view of entitlement status, seat usage, and contract validity across FortiSASE-Sovereign, FortiAnalyzer, and FortiGate services.

Navigating the License Dashboard

To access the licensing overview, select License from the left-hand navigation menu. The dashboard is divided into specific product tabs:

- Sovereign SASE: View user licensing and cloud orchestrator status.
- FortiAnalyzer: Monitor logging and analytics entitlements.
- FortiGate: Manage hardware or virtual machine licenses integrated with the sovereign stack.

Monitoring User Licensing

Under the FortiSASE Sovereign User Licensing section, you can track real-time consumption:

- License Serial Number: The unique identifier for your SASE instance (e.g., FEMSSSTM26090091).
- Users (Assigned/Total): Displays the current utilization ratio. For example, 110 / 1.5K indicates 110 seats are currently provisioned out of a total capacity of 1,500.
- Contract Details: The table lists individual contract numbers, their specific seat counts, and the Start/End Dates.

Cloud Orchestrator & Web Portal

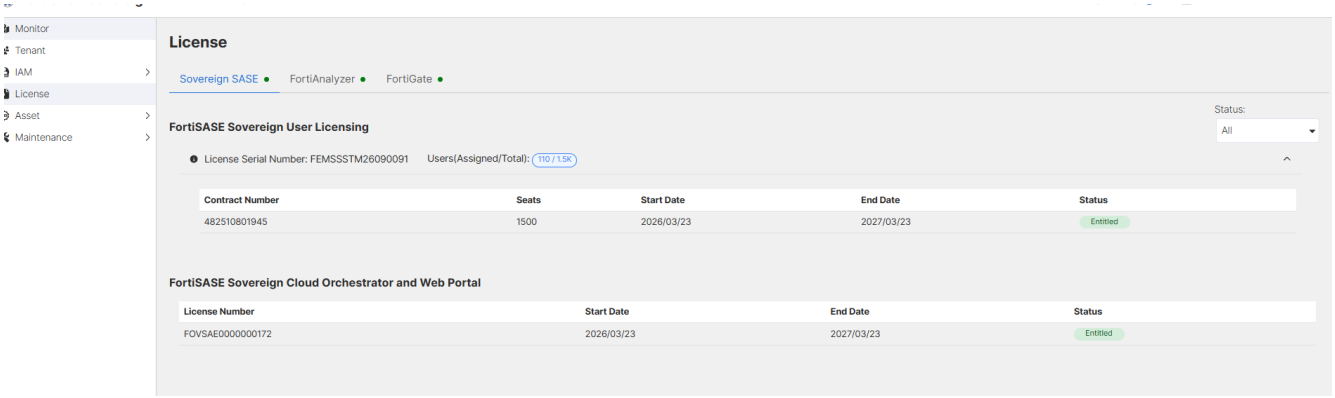
The FortiSASE Sovereign Cloud Orchestrator section confirms the validity of your management interface.

- Ensure the Status is marked as Entitled to maintain access to the web portal and configuration tools.
- Check the End Date regularly to avoid service disruption.

Status Definitions

You can filter licenses using the Status dropdown menu:

- Entitled:The license is active and currently within its validity period.
- Expiring:The contract is nearing its end date; renewal is recommended soon.
- Expired: The contract has ended. Services associated with this license may be restricted.
- Upcoming: A purchased license that has been registered but the start date has not yet been reached.
- Invalid:The contract has been decomissioned.



Maintenance

Upgrade

System upgrades for FortiSASE-Sovereign are managed through a coordinated process between Organization Administrators and the DevOps team. This page is used to finalize and manage the schedule once an upgrade has been initiated on the backend.

The Upgrade Workflow

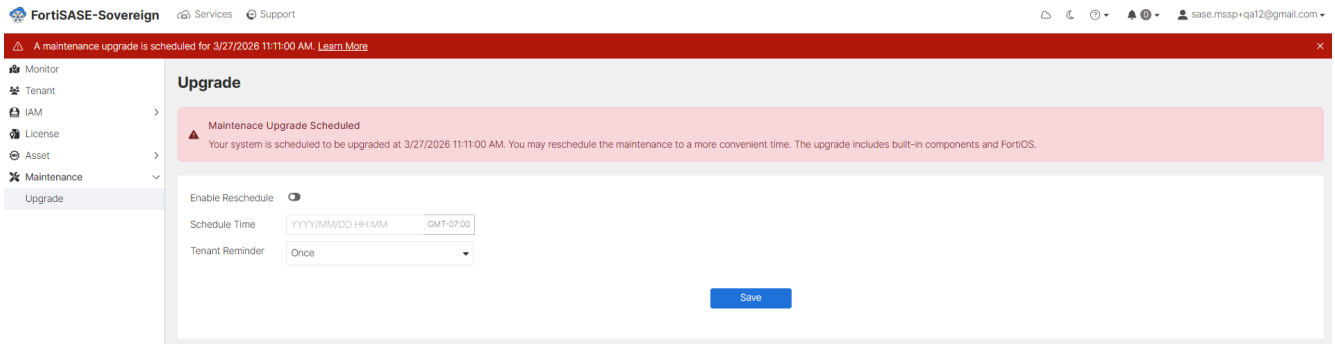
Unlike standard automated updates, the platform follows an "On-Demand" flow:

1. Request: The Administrator contacts the DevOps/Support team to request a system upgrade.
2. Trigger: DevOps triggers the upgrade notification from the backend.
3. Confirmation: A notification banner appears in the portal: "A maintenance upgrade is scheduled for [Date/Time]."

Finalizing the Schedule

Once the upgrade notification is active, you have the authority to adjust the maintenance window to fit your operational needs:

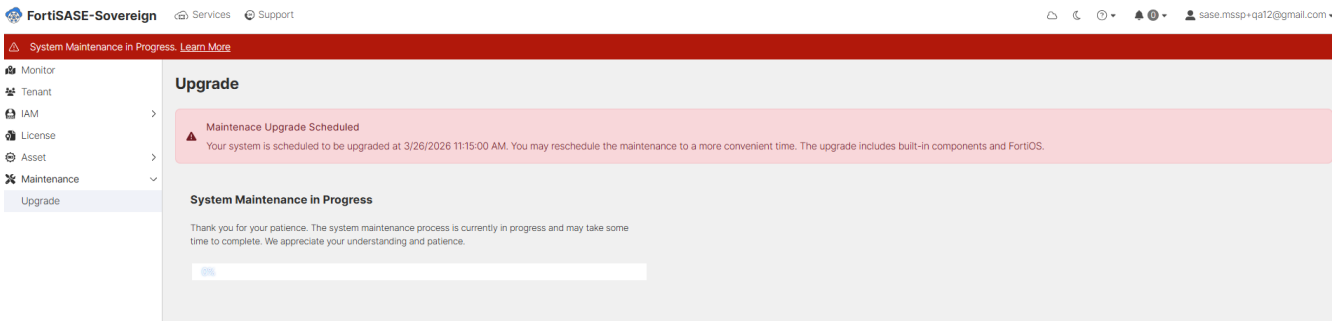
- Review Proposed Time: Check the Maintenance Upgrade Scheduled card for the initial time proposed by the system/DevOps.
- Rescheduling: If the proposed time conflicts with business hours:
  a. Toggle Enable Reschedule to On.
  b. Input a new Schedule Time (Format: YYYY/MM/DD HH:MM).
  c. Click Save.
- Note: The upgrade will execute automatically at the confirmed time. Ensure all stakeholders are informed.



Tenant Communication

Since upgrades may involve brief service interruptions for built-in components and FortiOS, use the Tenant Reminder tool to automate alerts:

- Setup: Select a reminder frequency (e.g., Daily or Weekly) from the dropdown menu.
- Delivery: The system will notify all sub-tenants regarding the upcoming maintenance window you have scheduled.

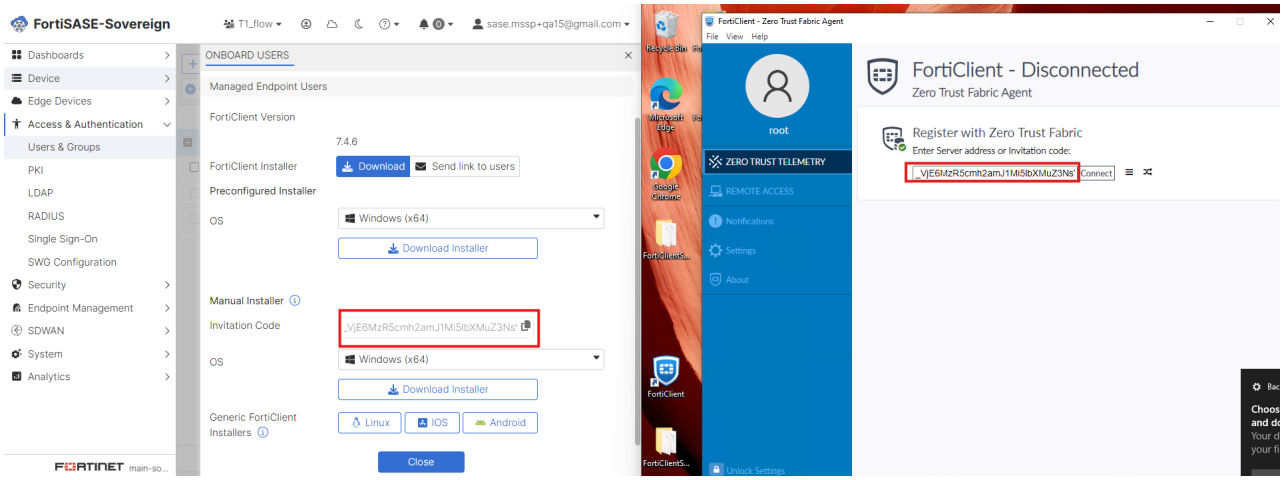


IPsec Secure Internet Access

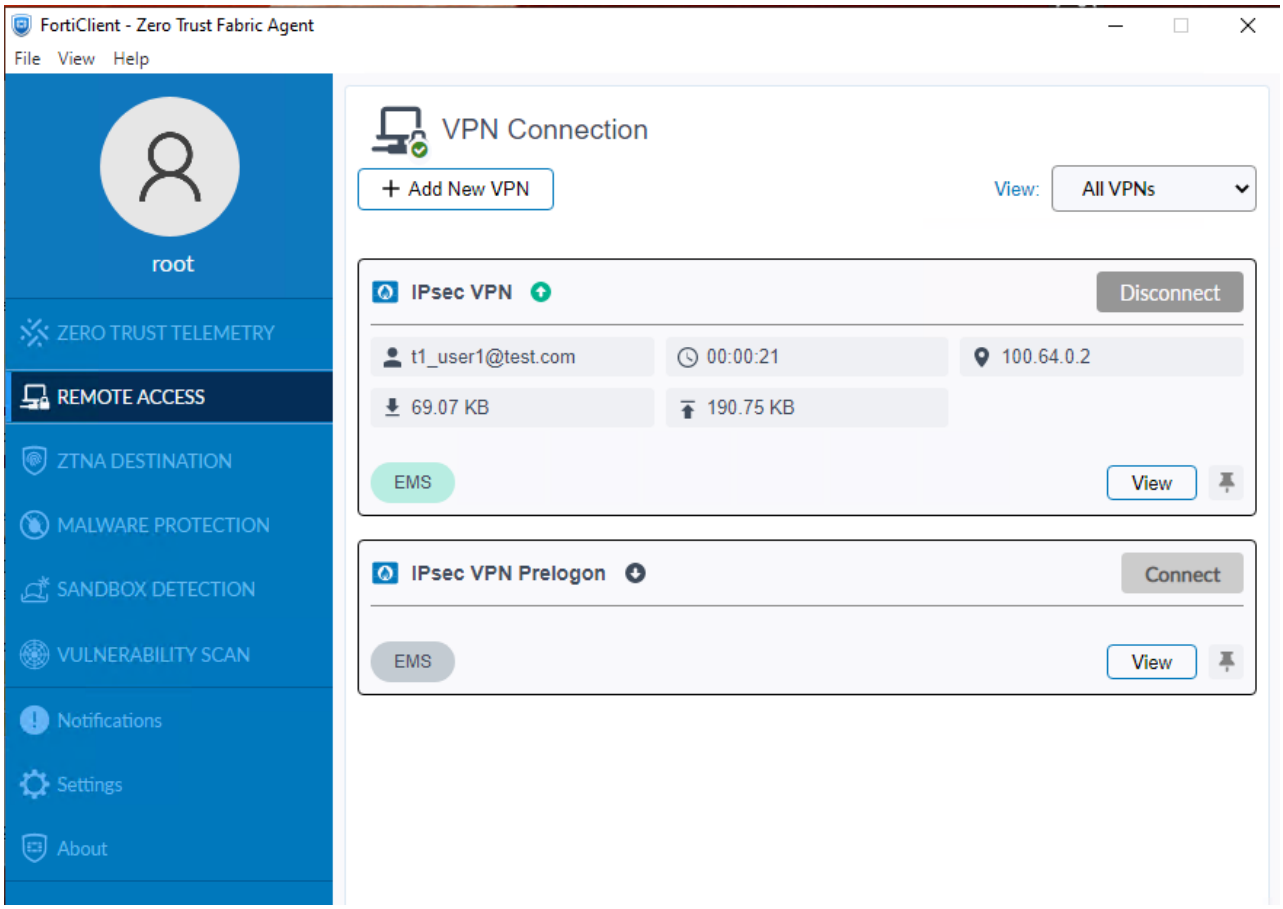
FortiSASE-Sovereign supports agent-based remote user connectivity using IPsec Version 2.

To support IPsec for remote agents:

- Remote users must install FortiClient 7.4 or higher on their endpoints, as needed. Please refer to FortiSASE-Sovereign release note for supported platforms and FortiClient versions.
- Administrators must configure and use single sign on, RADIUS, or local authentication for user authentication. Refer to Access & Authentication.
- Endpoints must be onboarded to receive secure tunnel configurations. This can be done by administrator sharing FortiSASE-Sovereign invitation code to user whose endpoint is preconfigured with a supported FortiClient Version. Local users configured on FortiSASE-Sovereign will also receive an email with the invitation code.



- User will receive two tunnel configurations, IPsec VPN and IPsec VPN Prelogon. For Secure Internet Access, connect IPsec VPN with local user, RADIUS user or single sign on user.



FortiSASE-Sovereign supports these features for IPsec remote agents:

- IPsec VPN auto connect. This can be enable/disable per endpoint management profile under Endpoint Management > Profile >.
- IPsec VPN always on. This can be enable/disable per endpoint management profile under Endpoint Management > Profile.
- VPN Split tunneling. This can be configured per endpoint management profile under Endpoint Management > Profile.
- Security policies.
- Split DNS. This can be configured under Endpoint Management > DNS. This feature is only supported for endpoints matched by proxy-based security policies and security profiles.
- Split DNS

Considerations

- LDAP authentication is unavailable for remote agents using IPsec.

Security

Policies

You must associate any traffic going through FortiSASE-Sovereign with a policy. Policies control where the traffic goes, how FortiSASE-Sovereign processes it, and whether or not FortiSASE-Sovereign allows it to pass through.

When a session is initiated through the VPN tunnel, FortiSASE-Sovereign analyzes the connection and performs a VPN policy match. FortiSASE-Sovereign performs the match from top down and compares the session with the configured VPN policy parameters. When there is a match and the action is Accept, FortiSASE-Sovereign applies the enabled security components to the traffic. If the action is Deny, FortiSASE-Sovereign blocks the traffic from proceeding.If the action is Isolate, FortiSASE-Sovereign isolates the traffic in a remote container with content rendered safely to the end user.

Default Policies

FortiSASE-Sovereign is configured with the following default VPN policies:

VPN policy	Description
Allow-All	Allows traffic for all services for all VPN users. You can edit and delete this VPN policy.
Implicit Deny	Denies access to traffic that does not match another configured VPN policy. You cannot edit or delete this VPN policy.

With only these default VPN policies and no custom configurations, FortiSASE Sovereign allows traffic to pass through the Allow-All VPN policy, and applies the enabled security components for scanning and processing.

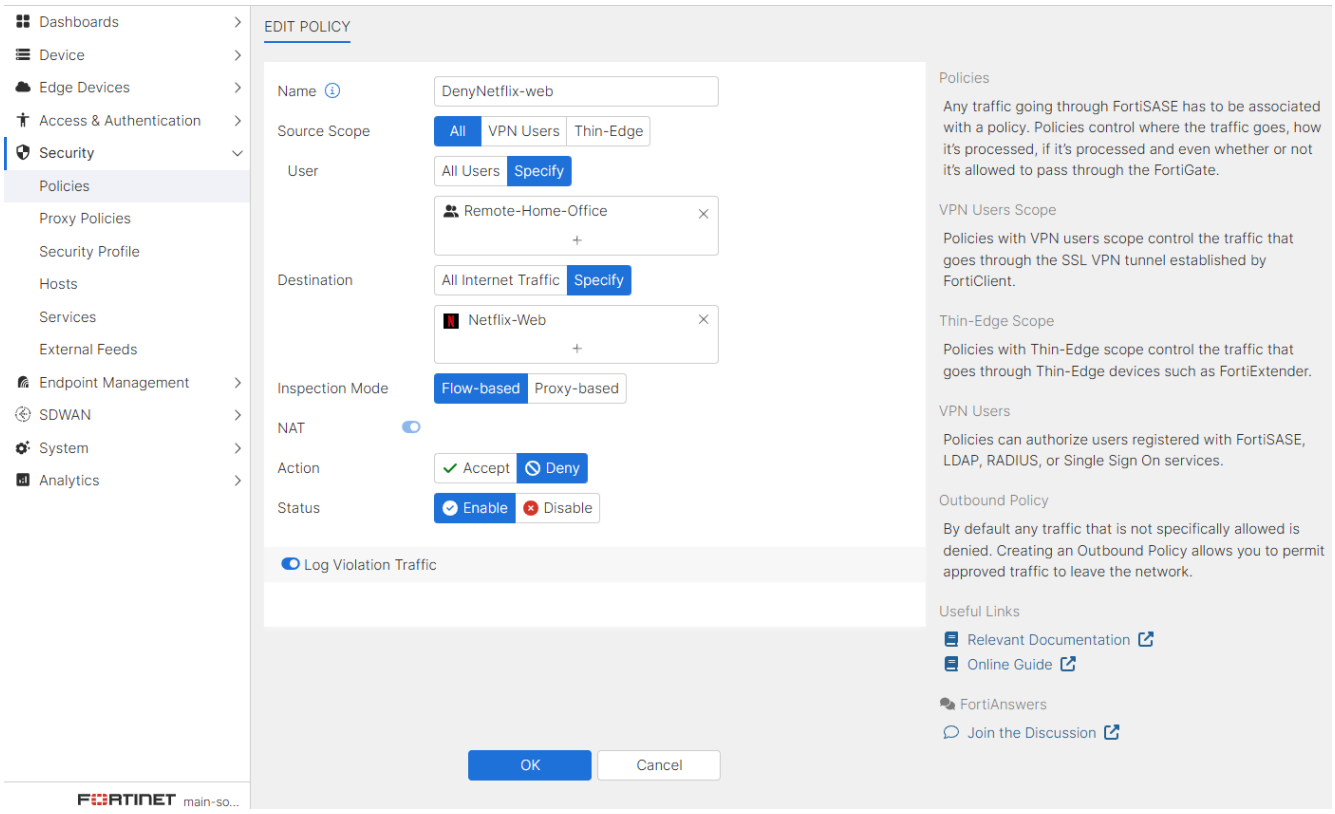
Adding policies to perform granular firewall actions and inspection

You can add multiple policies to perform granular firewall actions and inspection. This example configures a policy to block a set of remote users access to all Netflix-Web traffic.

The following provides instructions for configuring the described policies. You may want to configure similar policies, modifying settings based on your environment.

To add policies to perform granular firewall actions and inspection:

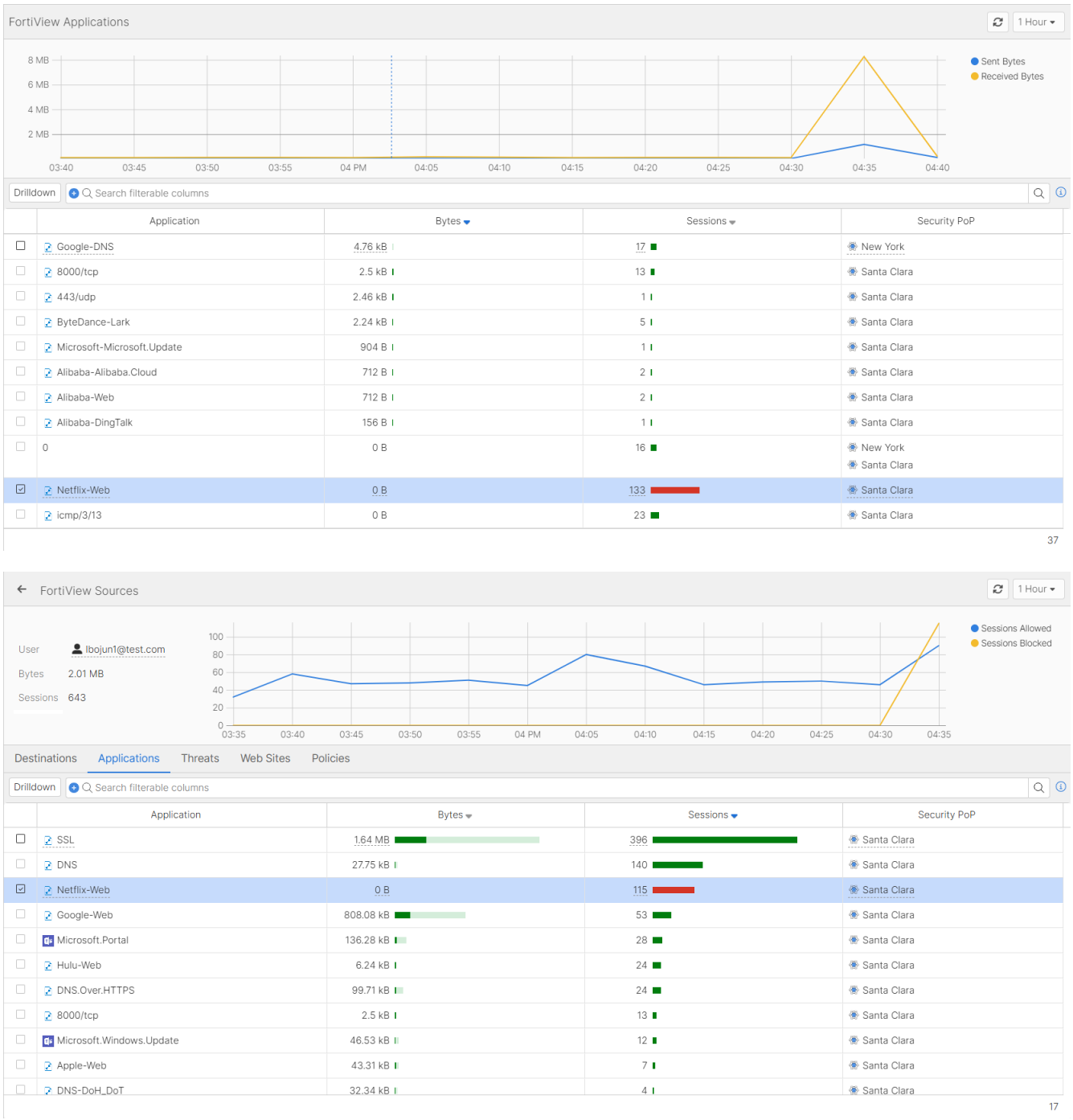
1. Go to Security > Policies.
2. Create the DenyNetflix-web policy:
   a. Click Create.
   b. In the Name field, enter DenyNetflix-web.
   c. For Source Scope, select Specify.
   d. Click +, and select the Remote-Home-Office user group from the Select Entries pane.
   e. In the Destination field, select Specify, then do the following:
      i. Click +.
      ii. Select Infrastructure.
      iii. In Select Entries panel, search “Netflix-Web”.
      iv. Select it and click Close.
   f. In the Action field, select “Deny”
   g. Leave all other fields at their default values.
   h. Click OK.



In VPN and secure web gateway policies, when you select an infrastructure in the Destination field, you cannot select hosts and services, and vice-versa.

When a session is initiated through the VPN tunnel, FortiSASE Sovereign analyzes the connection and performs a policy match. FortiSASE Sovereign performs the match from top down and compares the session with the configured policy parameters. For example, consider that a user who belongs to the Remote-Home-Office user group attempts to access Netflix-Web. FortiSASE Sovereign attempts to match the DenyNetflix-web, the traffic is for *.netflix.com. Then, FortiSASE Sovereign attempts to match this policy success. FortiSASE Sovereign denies the user access to www.netflix.com.

You can view data for access attempts on the FortiView Sources dashboard. You can view the application, destination, and policy information.



Security Profile

Security profile groups

You can create security profile groups, which allow you to group different security profile settings together. You can then configure the profile group as part of a policy.

This topic covers the following use cases:

- Security profile groups for VPN users
- Security profile groups for SWG users

Security profile groups for VPN users

To create a security profile group and configure it in a VPN policy:

1. Go to Security > Security Profile. By default, the Internet Access tab is selected in the top right corner. (If you have configured secure private access, you can select between the Internet Access or Private Access tabs to select which traffic the security profile group applies to.)
2. From the Profile Group dropdown list in the top right corner, click +.
3. In the Name field, enter the desired name.
4. Select Feature Set, “Flow-based” used for flow type Profile, “Proxy-based” used for proxy type Profile.
5. In the Initial Configuration field, do one of the following:
   a. Select Default to configure the new group with the same settings as the default security profile group.
   b. Select Based On to configure the new group with the same settings as an existing non-default security profile group. From the dropdown list, select the desired group.
6. Click OK.
7. Configure the profile group in a VPN policy:
   a. Go to Security > Policies.
   b. Select your desired policy.
   c. In the Profile Group field, select Specify. From the dropdown list, select the created object. The Profile Group field is only available for policies where the Action is configured as Accept.
   d. Click OK.

Security profile groups for SWG users

For SWG users, the process for configuring a security profile group and policy is similar to the process for configuring these settings for VPN users.

The only difference is that these steps are required if SSO authentication is used for SWG users:

- You must configure SSL inspection in Configure SSL ensuring that Deep Inspection is selected.
- You will need to download the CA certificate and install it on endpoints.

Endpoint Management

Profile

FortiSASE-Sovereign supports multiple endpoint profiles to provide granular behavior for different user types that belong to an Active Directory (AD) group or a non-AD group, such as:

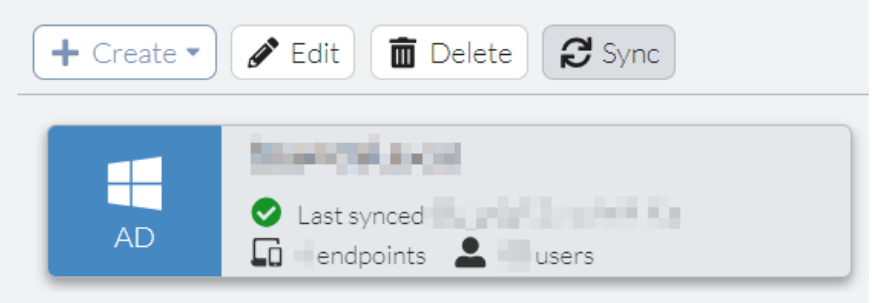
- IT can disconnect from always-on tunnels.
- Marketing can use removable media and authenticates using LDAP.
- All other users cannot disconnect from always-on tunnels or use removable media, and authenticate using single sign on (SSO).

Endpoint Management > Profile presents a table of profiles, with the Default profile assigned to all other users if you have not defined custom profiles. You cannot delete the Default profile.

You can prioritize and assign endpoint profiles to on-net endpoints based on matching AD domain users and groups or you can assign endpoint profiles based on endpoints assigned to different non-AD groups.

Viewing users and groups from an AD server requires an AD connection in Endpoint Management > Domain.

In Endpoint Management > Domain, click an AD domain card and click Sync to synchronize the AD connection with any updates from the AD server, if necessary:



When creating a new endpoint profile, you can use the Groups & AD Users tab to select which AD users/groups or non-AD groups you will apply the profile to. To assign endpoints to different non-AD groups, see Groups & AD Users.

To configure Profiles options:

1. Go to Endpoint management > Profile.
2. Do one of the following:
   - Click Create to create a new endpoint profile. In the Name field, enter the desired name of the endpoint profile.
   - To modify an existing endpoint profile, select the profile, then click Edit.
3. Configure the options on each tab as the following topics describe:
   - Access
   - Protection

- Sandbox
- ZTNA
- Groups & AD Users

4. Click OK to save the endpoint profile.
5. (Optional) Once you have configured an endpoint profile, you can clone it to quickly create additional endpoint profiles. This feature is useful when setting up multiple profiles with slight variations while maintaining a consistent baseline configuration. To clone an existing endpoint profile, do the following:
   a. Select an existing endpoint profile and click Edit > Clone.
   b. In the Name field, enter the desired name.
   c. Click OK.

Considerations

When the FortiSASE-Sovereign Endpoint Management Service uses AD servers with Groups & AD Users for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the Server address in the AD connection and may require some configuration or topology changes.

Access

To configure the Access tab:

1. Create a new profile or edit an existing one:
   a. Go to Endpoint management > Endpoint profiles. By default, the Profiles tab is selected.
   b. Click Create or edit an existing profile.
   c. If creating a new profile, in the Name field, enter the desired name of the endpoint profile.
2. On the Access tab:
   - Enable the toggle for Show tags on FortiClient to display ZTNA tags on FortiClient profile tab for managed endpoints, or disable the toggle to hide ZTNA tags on FortiClient.
   - Enable the toggle for Notify endpoint of VPN connectivity issues to allow FotiClient to pop notifications to endpoints when the status of FortiSASE-Sovereign Cloud Security tunnel changes, or disable the toggle to mute FortiClient notifications for tunnel events.
   - To enable autoconnect to the FortiSASE-Sovereign Cloud Security tunnel, enable Auto Connect to FortiSASE-Sovereign, or disable it to allow endpoints to connect to FortiSASE-Sovereign Cloud Security tunnel manually.
   - Enable the toggle for Force Always On VPN to prevent endpoints from being able to disconnect from the FortiSASE-Sovereign Cloud Security tunnel, or disable it to allow endpoints to disconnect using a Disconnect button on FortiClient.
   - Configure the remaining options as the following topics describe:
   - Pre-logon authentication
   - On/off-net Settings
   - Bypass FortiSASE-Sovereign

3. Click OK to save endpoint profile.

Pre-logon authentication

Under Advanced settings, you can enable Pre-logon authentication for a profile. See Global connection settings for details.

On/off-net Settings

On-net rule sets determine if FortiSASE-Sovereign considers endpoints trusted or on-net, meaning they are in a corporate network that has some level of on-premise security and do not need to automatically connect to FortiSASE-Sovereign tunnel for security inspection. This also helps to optimize FortiSASE-Sovereign bandwidth usage.

For example, by configuring an on-net rule set that uses your corporate network's public IP address, any endpoints behind this corporate network do not autoconnect to the FortiSASE-Sovereign Cloud Security tunnel. Instead, endpoints only autoconnect when their public IP addresses do not match the configured public IP address in the on-net rule, indicating they are untrusted or off-net and enforcing security inspection via FortiSASE-Sovereign SIA.

FortiSASE-Sovereign supports on-net rule sets with the following detection types to determine if an endpoint is connecting from a trusted location:

Detection type	Description
Connects with a known public IP	In the Known public (WAN) IP addresses field, enter the desired IP address. You can configure multiple addresses using the + button. FortiSASE-Sovereign supports configuration of single IP addresses and IP subnets. FortiSASE-Sovereign considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified.
Is connected to a known DNS server	In the Known server IP addresses field, configure at least one IP address for the desired DNS server. You can configure multiple IP addresses using the + button. FortiSASE-Sovereign considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration.
Is connected to a known DHCP server	If you enable Identify servers by IP/MAC addresses, configure the IP and/or MAC address for the desired DHCP server in the Known server IP addresses and Known MAC addresses fields, respectively. If configuring Identify servers by IP/MAC addresses, the MAC Address field is optional. If you enable Identify servers by DHCP option 224, configure the DHCP code for the desired DHCP server. If the DHCP server is a FortiGate, you can use the FortiGate serial number as the DHCP code, if desired. Otherwise, the DHCP code can be any string configured in the DHCP server as option 224.

Detection type	Description
	You can configure Identify servers by IP/MAC addresses, Identify servers by DHCP option 224, or both. You can configure multiple IP and MAC addresses and DHCP codes using the + button on each tab.
Connects from a known local subnet	In the Known subnets field, enter an IP address range. In the Known gateway MAC addresses field, optionally enter the default gateway MAC address. You can configure multiple addresses using +. FortiSASE-Sovereign considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified and if its default gateway MAC address matches the one specified, if it is configured.
Can ping a known server	In the Known server IP addresses field, enter the server IP address. You can configure multiple addresses using +. FortiSASE-Sovereign considers the endpoint as satisfying the rule if it can access the server at the specified IP address.

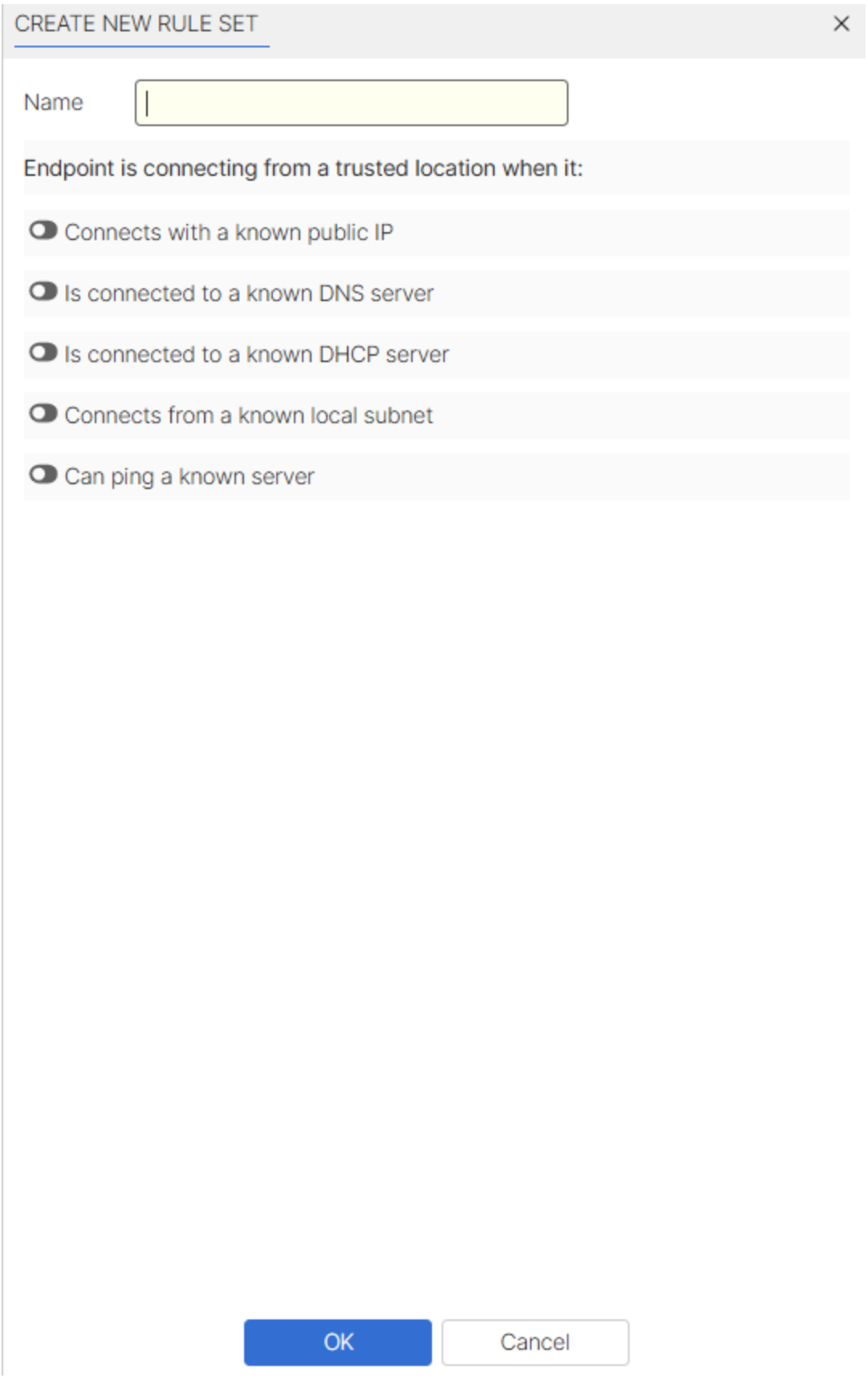
Logic used for multiple rules within a rule set:

- If you configure rules of multiple detection types for a rule set, the endpoint must satisfy all configured rules (AND logic condition) to satisfy the entire rule set.

Logic used for multiple conditions within a rule:

- For most rules, if you configure multiple conditions, then the endpoint needs to satisfy only one of them (OR logic condition) to satisfy the rule. An exception to this is when Connects from a known local subnet is enabled where both Known subnets and Known gateway MAC addresses are specified. In this case, only one of the multiple known subnets specified (OR logic condition) and one of the known gateway MAC addresses (AND logic condition) is required is satisfy the rule.

To configure on/off-net settings:


CREATE NEW RULE SET
Name
Endpoint is connecting from a trusted location when it:
Connects with a known public IP
Is connected to a known DNS server
Is connected to a known DHCP server
Connects from a known local subnet
Can ping a known server
OK
Cancel

1. In the desired profile, on the Access tab, under On/off-net Settings, set On/off-net detection to Enable.

   To configure an on-net rule set to prevent autoconnect to the FortiSASE-Sovereign Cloud Security tunnel when endpoints are on-net, do the following:

   On-net rule sets can also be created, edited, and deleted in Endpoint management > Profile from the On-net rule sets tab. From this tab, you can also view which profiles each rule set is used in.

   a. Set On/off-net detection to Enable.
   b. From the On-net rule set dropdown list, click + to create a new on-net rule set.
   c. In the Create new rule set slide-in, select one or more detection types by toggling them.
   d. Configure the required fields as described for each detection type.
   e. Click OK to save the on-net rule set.
   f. Click OK on the confirm prompt to select the newly created on-net rule set.
   g. Enable Exempt endpoint from FortiSASE-Sovereign auto-connect when endpoint is on-net.

Considerations

Exempt endpoint from FortiSASE-Sovereign auto-connect when endpoint is on-net is designed to prevent FortiSASE-Sovereign from automatically establishing a secure connection (SIA) when the endpoint is already within the trusted and secured corporate network (i.e. on-net). This is useful for reducing unnecessary SIA bandwidth usage and ensuring traffic is routed directly through corporate firewall when the endpoint is already behind one. However, the exemption mechanism is event-driven and only takes effect after specific system-level or network events occur on the endpoint that include: system login/logout, system power on/off, system restart, network reset, or change in network status.

Thus, if an off-net endpoint that is already connected to FortiSASE-Sovereign via the FortiSASE-Sovereign Cloud Security tunnel transitions to an on-net status without triggering any of the aforementioned events, the autoconnect exemption is not immediately applied. In such cases, the endpoint continues to stay connected to FortiSASE-Sovereign even though it is on-net.

Bypass FortiSASE-Sovereign

You can configure split tunneling destinations to optimize FortiSASE-Sovereign bandwidth by excluding trusted traffic from flowing through the FortiSASE-Sovereign Cloud Security tunnel. Such traffic is redirected to the endpoint's physical interface, bypassing FortiSASE-Sovereign. For example, you can add high-bandwidth applications like Microsoft Teams or Zoom as split tunneling destinations.

To configure split tunneling destinations:

1. Go to Endpoint management > Profile.
2. In the desired profile, on the Access tab, under Bypass FortiSASE-Sovereign, click Create.
3. Configure the following fields:

Option	Description
Type	Select Infrastructure, FQDN, Local Application, or Subnet.
Match	• If you selected Infrastructure, select the desired application from the dropdown list. • If you selected FQDN, enter or select the desired fully qualified domain name (FQDN).

Option	Description
	The FQDN resolved IP address is dynamically added to the route table when in use and removed after disconnection. For example, to exclude YouTube from the tunnel, enter youtube.com. When endpoint users use any popular browser such as Chrome, Edge, or Firefox to access youtube.com, this traffic does not go through the tunnel. • If you selected Local Application, specify an application using its process name, full path, or the directory where it is installed. When entering the directory, you must end the value with \. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%, %programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. You can add multiple entries by separating them with a semicolon. For example, to exclude Microsoft Teams and Firefox from the tunnel, enter any of the following combinations: • Application Name: teams.exe;firefox.exe • Full Path: C:\Users\<username>appData\Local\Microsoft\Teams\current\Teams.exe;C:\Program Files\Mozilla Firefox\firefox.exe • Directory: C:\Users\<username>appData\Local\Microsoft\Teams\current\;C:\Program Files\Mozilla Firefox\ To find a running application's full path, on the Details tab in Task Manager, add the Image path name column. • If you selected Subnet, enter the desired subnet. The subnet is dynamically added to the route table when in use and removed after disconnection. You can select host groups when using the Subnet match type. You must create host groups in Security > Hosts before they become visible in the Create Destination dialog. • For FortiSASE instances with SSL remote agent connectivity: • You can select host groups when using the Subnet match type. You must create host groups in Security > Hosts before they become visible in the Create Destination dialog. • You can only configure a Subnet or IP range steering bypass destination for the Default endpoint profile. All custom endpoint profiles inherit and apply the subnet destinations defined in the Default profile. • For FortiSASE with IPsec remote agent connectivity: • You can only configure the subnet using the input field in the Create Destination dialog. • You can configure unique Subnet steering bypass destinations for custom profiles and the Default profile.

4. Click OK.

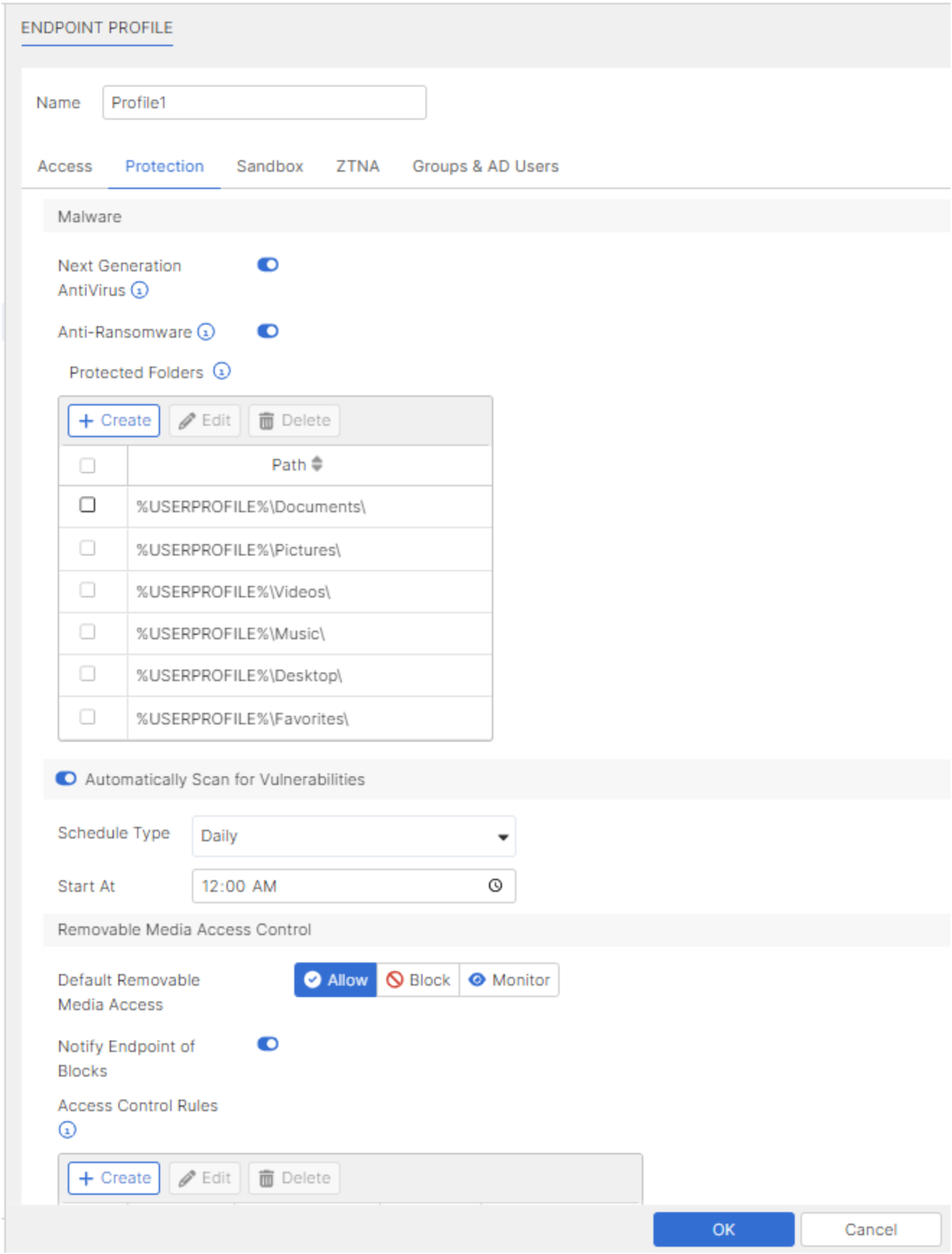
Considerations

- Windows FortiClient endpoints support application-based split tunneling or full tunneling with FortiSASE. FortiClient endpoints on other platforms support full tunneling. See Supported FortiClient features.

- FortiSASE-Sovereign does not support wildcard FQDNs when configuring an FQDN split tunneling destination.

Protection

To configure the Protection tab:


ENDPOINT PROFILE
Name
Profile1
Access
Protection
Sandbox
ZTNA
Groups & AD Users
Malware
Next Generation AntiVirus
Anti-Ransomware
Protected Folders
Create
Edit
Delete
Path
%USERPROFILE%\Documents\
%USERPROFILE%\Pictures\
%USERPROFILE%\Videos\
%USERPROFILE%\Music\
%USERPROFILE%\Desktop\
%USERPROFILE%\Favorites\
Automatically Scan for Vulnerabilities
Schedule Type
Daily
Start At
12:00 AM
Removable Media Access Control
Default Removable Media Access
Allow
Block
Monitor
Notify Endpoint of Blocks
Access Control Rules
Create
Edit
Delete
OK
Cancel

1. Create a new profile or edit an existing one:
   a. Go to Endpoint management > Profile. By default, the Profiles tab is selected.
   b. Click Create or edit an existing profile.
   c. In the Name field, enter the desired name of the endpoint profile.
2. On the Protection tab, in Malware, configure the following:
   a. Enable Next Generation AntiVirus. This feature includes real-time protection against viruses, as well as cloud-based malware detection. Cloud-based malware protection protects endpoints from high risk file types from external sources such as the internet or network drives by querying FortiGuard to determine whether files are malicious. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.
   b. Enable Anti-Ransomware. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient. Antiransomware protects all content in the selected folders against unauthorized changes. You can click Create to add a custom directory. To remove a folder, select it then click the Delete button.
3. FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities and the ability to automatically patch vulnerabilities with the configured minimum severity level. You can view a summary of endpoint vulnerability information on the Dashboard.

   On the Protection tab, in Automatically Scan for Vulnerabilities:
   a. Enable Scheduled scanning and select these settings:
      i. For Schedule type, select Weekly (default), Daily, or Monthly.
      ii. For Scan on, select Sunday (default), or specify a day from Monday through Saturday or 1st through 31st.
      iii. For Start at, specify the desired time to start the scan.
   b. On the Protection tab, in Removable Media Access Control, configure the following:

      For Default Removable Media Access Control, select Allow (default), Block, or Monitor. This feature only works for endpoints where Malware Protection was enabled when installing FortiClient.

      Enable Notify Endpoint of Blocks to display a bubble notification when FortiClient takes action with a removable media device.

      In Access Control Rules, click Create to create a removal media access rule. Configure the following fields. For the class, manufacturer, vendor ID, product ID, and revision, you can find the desired values for the device in one of the following ways:
      - Microsoft Windows Device Manager: select the device and view its properties.
      - USBDeview

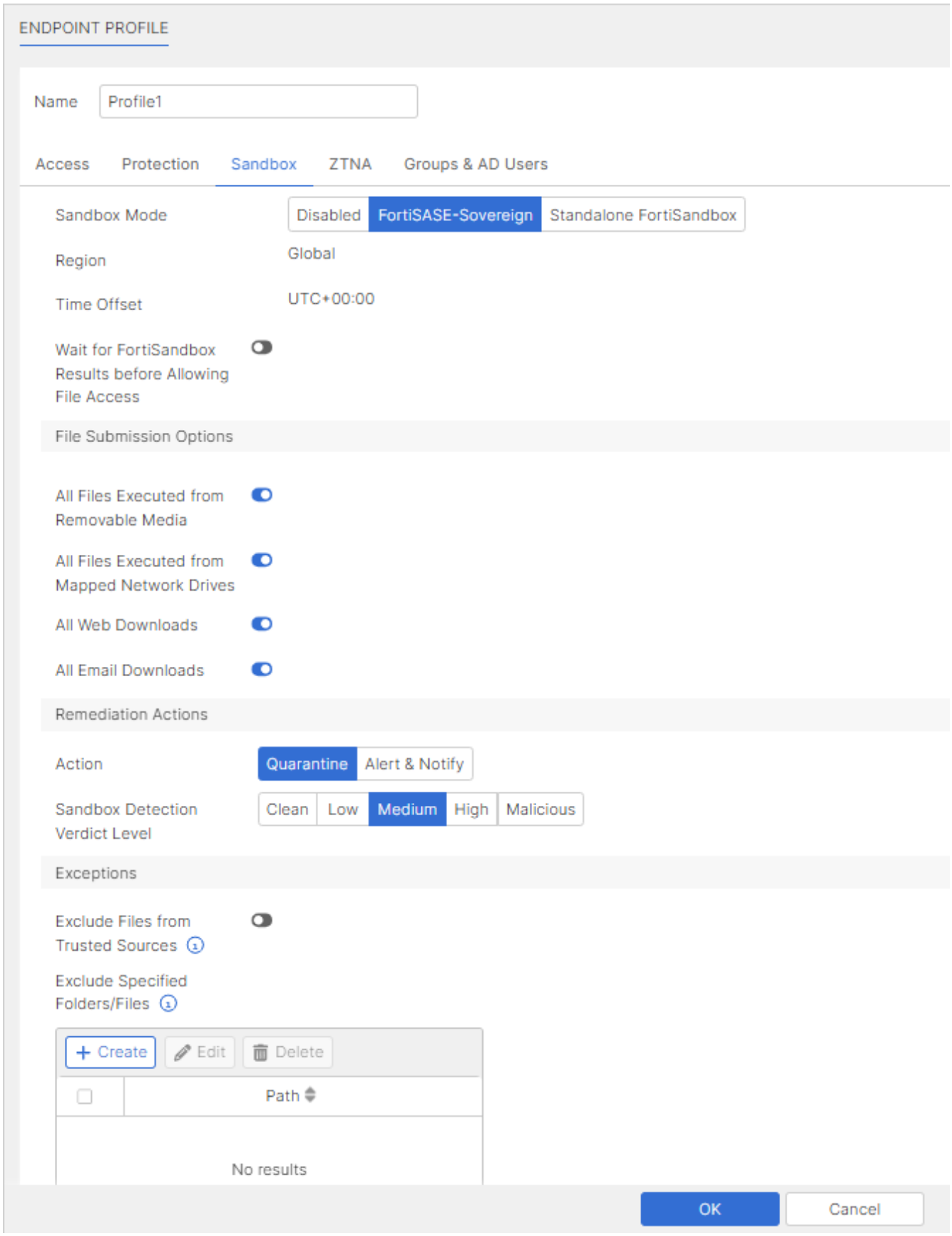
Option	Description
Type	Select Simple or Regex for the rule type. When Simple is selected, FortiClient performs case-insensitive matching against classes, manufacturers, vendor IDs, product IDs, and revisions. When Regex is selected, FortiClient uses Perl Compatible Regular Expressions (PCRE) to perform matching against classes, manufacturers, vendor IDs, product IDs, and revisions.
Action	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: • Allow: Allow access to removable media devices connected to the

Option	Description
	endpoint that match this rule. • Block: Block access to removable media devices connected to the endpoint that match this rule.
Class	Enter the device class.
Manufacturer	Enter the device manufacturer.
Vendor ID	Enter the device vendor ID.
Product ID	Enter the device product ID.
Revision	Enter the device revision number.

Click OK.

Sandbox

To configure the Sandbox tab:


ENDPOINT PROFILE
Name
Profile1
Access
Protection
Sandbox
ZTNA
Groups & AD Users
Sandbox Mode
Disabled
FortiSASE-Sovereign
Standalone FortiSandbox
Region
Global
Time Offset
UTC+00:00
Wait for FortiSandbox Results before Allowing File Access
File Submission Options
All Files Executed from Removable Media
All Files Executed from Mapped Network Drives
All Web Downloads
All Email Downloads
Remediation Actions
Action
Quarantine
Alert & Notify
Sandbox Detection Verdict Level
Clean
Low
Medium
High
Malicious
Exceptions
Exclude Files from Trusted Sources
Exclude Specified Folders/Files
Create
Edit
Delete
Path
No results
OK
Cancel

1. Create a new profile or edit an existing one:
   a. Go to Endpoint management > Profile. By default, the Profiles tab is selected.
   b. Click Create or edit an existing profile.
   c. In the Name field, enter the desired name of the endpoint profile.
2. On the Sandbox tab, configure the following. This feature only works for endpoints where Sandbox Detection was enabled when installing FortiClient. Configure the following options:

Options	Description
Sandbox mode	Select FortiSASE to configure connection to FortiSASE Sandbox or Standalone FortiSandbox to configure connection to an on-premise standalone FortiSandbox.
IP address/Hostname	For a standalone FortiSandbox, enter the FortiSandbox IP address, FQDN, or hostname.
Authentication	Optional. Enable to configure credentials to communicate with a standalone FortiSandbox.
Username	Optional. Enter the FortiSandbox username. This option is only available for a standalone FortiSandbox.
Password	Optional. Enter the FortiSandbox password. This option is only available for a standalone FortiSandbox.
Region	FortiSASE-Sovereign Sandbox region.
Time Offset	FortiSASE-Sovereign Sandbox time offset.
Wait for FortiSandbox results before allowing file access	Have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds.
File submission options	
All files executed from removable media	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
All files executed from mapped network drives	Submit all files executed from mapped network drives.
All web downloads	Submit all web downloads.
All email downloads	Submit all email downloads.
Notification type	Choose one of the following notification levels: • Lite: Displays notification balloon only when FortiSandbox detects malware in a submitted file. • Full: Displays a popup for every file submission sent to FortiSandbox regardless of the result.
Remediation Actions	

Options	Description
Action	Choose Quarantine or Alert & Notify for infected files. Whether FortiClient quarantines the file depends on if FortiSandbox reports the file as malicious and the Sandbox Detection Verdict Level setting.
Sandbox Detection Verdict Level	Select the desired detection verdict level. For FortiClient to apply the action selected in the Action field to an infected file, FortiSandbox must detect the file as this level or higher. For example, if Action is configured as Quarantine and FortiSandbox Detection Verdict Level is configured as Medium, FortiClient quarantines all infected files that FortiSandbox detects as Medium or a higher level (High or Malicious). FortiClient does not quarantine files for which FortiSandbox returns a verdict below this level (Low Risk or Clean).
Exceptions	
Exclude Files from Trusted Sources	Exclude files signed by trusted sources from FortiSandbox submission. Following is a list of sources that FortiSandbox trusts: • Microsoft • Fortinet • Mozilla • Windows • Google • Skype • Apple • Yahoo! • Intel
Exclude Specified Folders/Files	Click Create to exclude specified files/folders from FortiSandbox submission. You can use wildcards to specify file/folder exclusions.

Considerations

- When enabling Sandbox in an endpoint profile, and when using a FortiSASE-Sovereign-managed endpoint running FortiClient (macOS) and Microsoft Defender, you must enable passive mode on Microsoft Defender.
- FortiSASE-Sovereign Sandbox uses the FortiClient Cloud Sandbox service. See the FortiClient Cloud Sandbox (FortiSandbox SaaS) Service Description in the Fortinet Support portal.
  - For each endpoint, FortiClient can send a maximum of 300 files daily to FortiClient Cloud Sandbox (SaaS).
  - If multiple files are submitted around the same time, FortiClient sends one file to FortiClient Cloud Sandbox (SaaS), waits until it receives the verdict for that file, then sends the next file to FortiClient Cloud Sandbox (SaaS).
  - The file size limit is 100 MB.

    - When the daily limit is reached, FortiClient Cloud Sandbox (SaaS) sends a signal to the FortiClient endpoint to stop file submission to save resources on both sides.
- For a FortiSASE-Sovereign instance expecting heavy SMB traffic patterns with its agent remote users, to ensure optimal performance, for endpoint profiles with Sandbox mode set to FortiSASE-Sovereign, in Profile Configuration > Sandbox ensure the File submission options > All files executed from mapped network drives option is disabled.
- FortiSASE-Sovereign Sandbox only checks the following file types:

7z, arj, bz2, cpl, dll, doc, docm, docx, dot, dotm, dotx, exe, fla, flv, gz, jsfl, mht, mhtml, msi, ocx, odp, odt, pdf, pot, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, ps1, rar, rtf, swc, swf, swz, tar, thmx, xfl, xl, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, xps, xz, z, zip

ZTNA

Zero trust network access (ZTNA) application gateways and applications are key components in the FortiSASE-Sovereign ZTNA solution for agent-based remote users. A ZTNA application gateway serves as a secure entry point that mediates the connection between remote users and internal ZTNA applications. A ZTNA application represents the actual application or service that remote users attempt to access. A ZTNA application can be any internal web or enterprise application, cloud service, or on-premise resource. A ZTNA application gateway acts as a reverse proxy, ensuring that only authorized and compliant users can access ZTNA applications based on security policies that the organization defines. You can configure a FortiGate to serve as the ZTNA application gateway. See Zero Trust Network Access.

Once you configure ZTNA application gateways and applications, you can reference and use them in individual endpoint profiles.

To configure ZTNA application gateway on FortiSASE-Sovereign:

1. Go to Endpoint Management > ZTNA Application Catalogue.
2. Select the ZTNA Gateways Catalogue tab.
3. Click Create and enter following details for the ZTNA application gateway:

Field	Value
Alias	Enter a unique alias for your application gateway.
Address	Specify the IP address or FQDN of the FortiGate that is configured to act as the ZTNA application gateway.
Port	Specify the port number on the FortiGate that is designated for ZTNA.

To configure a ZTNA application on FortiSASE-Sovereign:

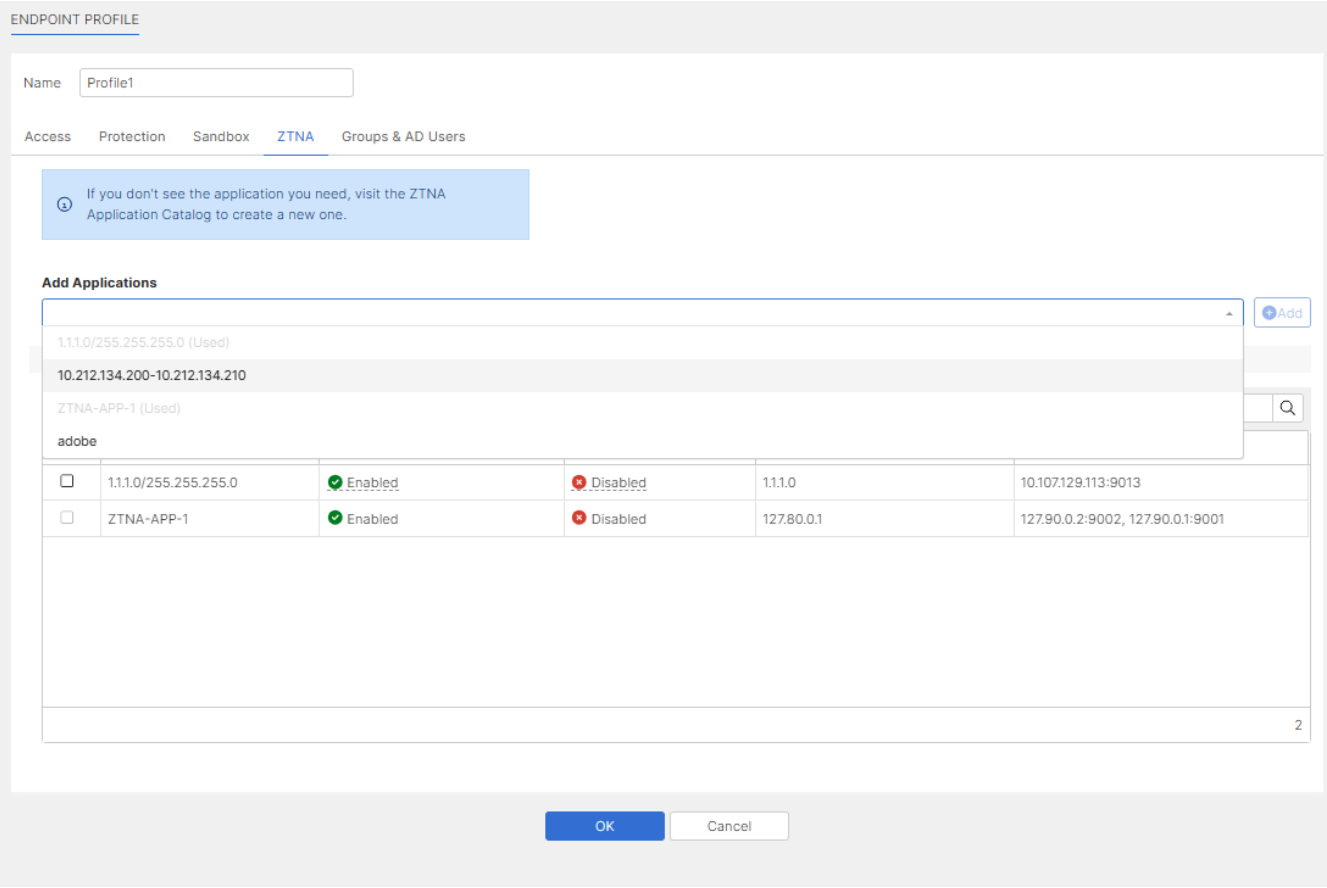
1. Go to Endpoint Management > ZTNA Application Catalogue.
2. Select the ZTNA Applications Catalogue tab.
3. Click Create to configure a new ZTNA application and enter the following details:

Field	Value
Application Name	Enter unique name for your application.

Field	Value
Application Type	Select IP, FQDN, or Wildcard FQDN. Additionally, for instances with supported FortiClient versions, select IP range or CIDR.
Address	Based on the Type selected, specify the IP address or FQDN of the ZTNA application. Additionally, for instances with supported FortiClient versions, specify the IP range, such as 192.168.1.1-192.168.1.100, or the CIDR, such as 192.168.1.0/24.
Port Type	Select Any or click Specify to enter a specific port number. Additionally, for instances with supported FortiClient versions, specify Port list to enter a list such as 80, 443, 8080 or Port range to enter a range such as 1000-2000.
Gateway	Click + to select the application gateway configured in earlier steps.

4. Click OK.

To use ZTNA application gateway and ZTNA application in endpoint profiles:



1. Create a new profile or edit an existing one:
   a. Go to Endpoint management > Endpoint profiles. By default, the Profiles tab is selected.
   b. Click Create or edit an existing profile.
   c. In the Name field, enter the desired name of the endpoint profile.
2. Select the ZTNA tab.
   a. User the Add Applications dropdown to select the ZTNA application.
   b. Click Add to add the application into ZTNA Applications List.
   c. Click OK.

Prerequisites

- For ZTNA applications, IP range and CIDR types, and Port list and Port range fields are visible in FortiSASE-Sovereign and supported for these versions of FortiClient:
  - FortiClient for Windows 7.2.8 or later

Groups & AD Users

To configure the Groups & AD Users tab:

1. Create a new profile or edit an existing one:
   a. Go to Endpoint management > Endpoint profiles. By default, the Profiles tab is selected.
   b. Click Create or edit an existing profile.
   c. In the Name field, enter the desired name of the endpoint profile.
2. On the Groups & AD Users tab, you can select Active Directory (AD) users, non-AD groups, or AD groups to assign the endpoint profile to.
3. Click Add and select AD Users or Groups as per your requirements:
   - When selecting AD Users, a slide-in appears, which allows you to view the domains corresponding to configured AD servers. You can select AD users from the list of AD users.
   - When selecting Groups, do one of the following:

Group type	Description
AD groups	A slide-in appears that allows you to view the domains corresponding to configured AD servers and select AD groups. To select AD user groups, you can collapse the LDAP domain using the + button and select the required AD groups from a tree view of groups using the toggle.
Non-AD groups	A slide-in appears that allows you to create nested non-AD user groups under Non-AD Groups and assign endpoints to the group. To configure a non-AD user group and add endpoints to the newly created non-AD group, do the following: Collapse Non-AD Groups using the + button. Select the group under that you want to create a group under and click Create sub-group.

Group type	Description
	Enter the Name of the group as desired. Select the available non-AD endpoints to add to the group. Click Add selected. Click OK. Only enable the toggle of the specific group to assign the profile to. Click OK.

Click OK.

Repeat step 3 to add more groups and AD users. If you add more groups to the list, the endpoint user must be a part of at least one group for FortiSASE-Sovereign to assign the profile to the endpoint.

Click OK to save the endpoint profile.

To view the endpoints that are assigned to a profile, click the profile and select View Endpoints from the toolbar.

Prerequisites

Viewing users and groups from an AD server requires configuring an AD connection in Endpoint Management > Domain. See Domain.

Considerations

- When the FortiSASE-Sovereign Endpoint Management Service uses AD servers with Groups & AD Users for endpoint profile assignments, these servers must use public IP addresses or publicly accessible FQDNs when configuring the Server address in the AD connection and may require some configuration or topology changes.
- FortiSASE-Sovereign only supports Create sub-group for non-AD groups and local AD groups. FortiSASE-Sovereign does not support this operation for Entra ID groups.
- FortiSASE-Sovereign cannot retrieve a user's Entra ID group membership information if the user belongs to more than 150 groups. As a workaround, you can apply an additional group filter in Entra ID to only send relevant groups in the SAML assertion to FortiSASE-Sovereign. See Technical Tip: Understanding the limitation of 150 assertions from Microsoft Azure as SAML IdP that may cause group mismatch in FortiGate. Although this article refers to FortiOS, the workaround applies to FortiSASE-Sovereign as well.

ZTNA Tagging

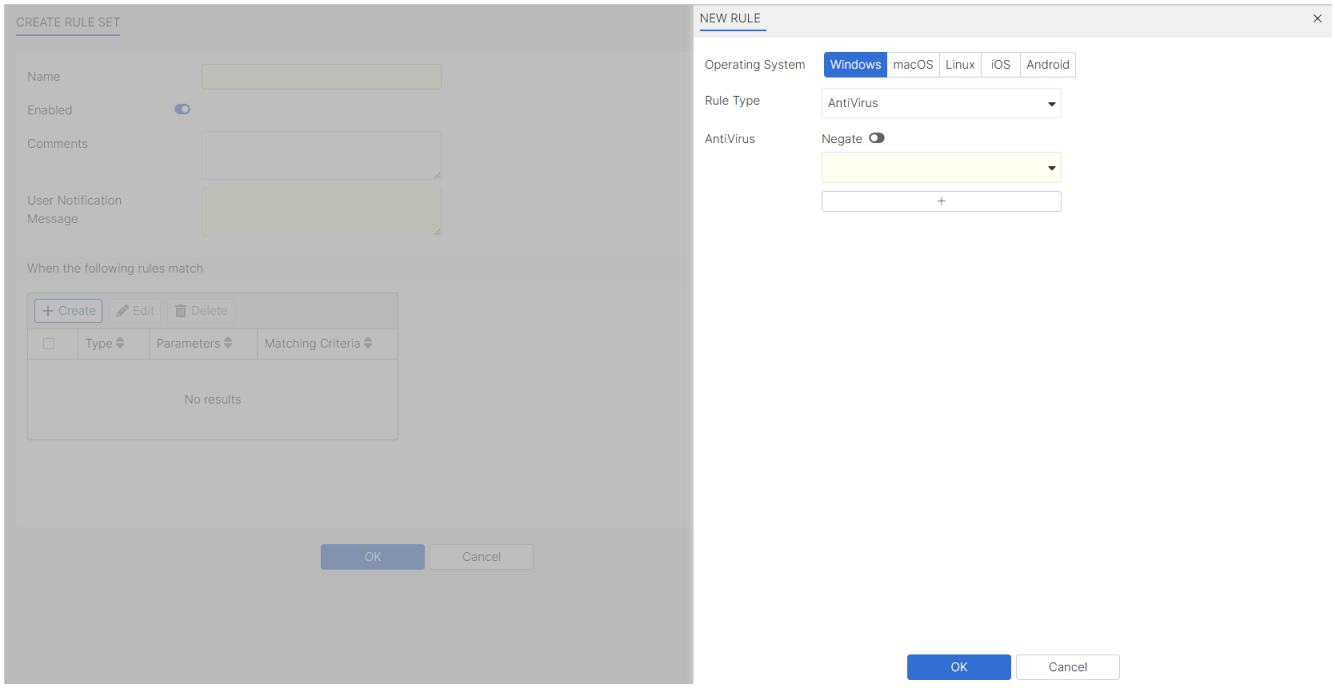
You can create security posture tags and tagging rules for Windows, macOS, Linux, iOS, and Android endpoints based on their OS versions, logged in domains, running processes, and other criteria. FortiSASE-Sovereign uses the security posture tagging rules to dynamically tag endpoints.

The following occurs when using tagging rules with FortiSASE-Sovereign and FortiClient:

1. FortiSASE-Sovereign sends tagging rules to endpoints.
2. FortiClient checks endpoints using the provided rules and sends the results to FortiSASE-Sovereign.
3. FortiSASE-Sovereign receives the results from FortiClient.
4. FortiSASE-Sovereign dynamically tags endpoints using the tag configured for each rule. You can view the dynamically tagged endpoints in Endpoint management > Managed Endpoints.

See Tagging Rule Types for descriptions of all tagging rule types.

Create Security Posture Tags and Tagging Rules



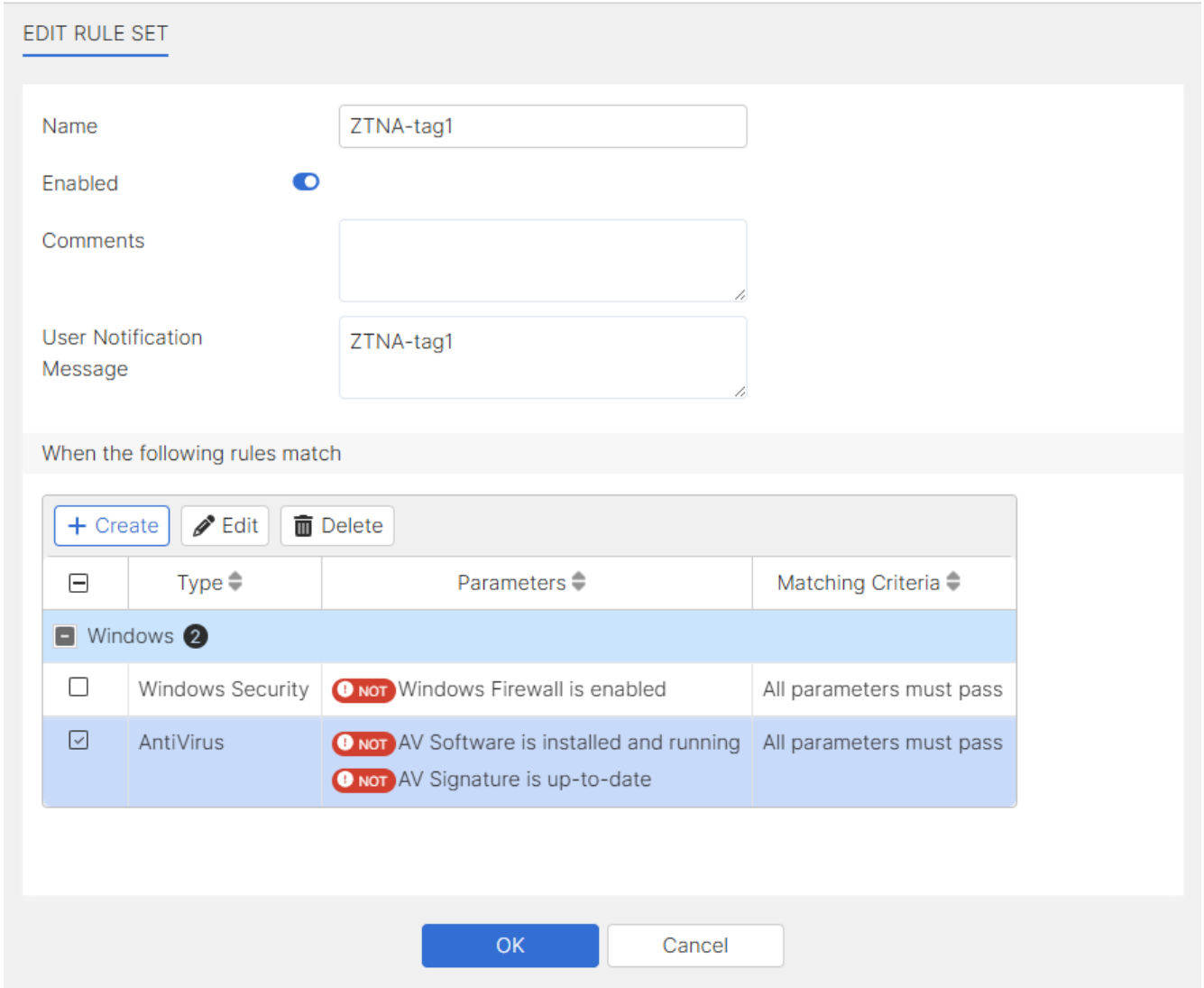
To configure Security posture tags and tagging rules in FortiSASE-Sovereign:

1. Go to Endpoint management > ZTNA Tagging.
2. Create a new security posture tag and tagging rule:
   a. In the ZTNA Tags tab, click Create.
   b. In the Name field, enter the desired rule set name.
   c. Toggle Enabled on or off to enable or disable the tag.

d. (Optional) In the Comments field, enter any desired comments.
e. In the User notification message, enter a message.
f. Configure a rule under When the following rules match:
   i. Click Create to create a tagging rule for the tag.
   ii. Select Operation System that rule applies to.
   iii. Select a suitable Rule Type, and configure its required options.
   iv. To add additional security posture tagging rules, repeat steps 1-3.
   v. Click OK to save the security posture tagging rule. A security posture tag with the same name will be created and applied to any endpoints matching the rule criteria.

Rule Logic Example

The following provides an example to assign a specific tag to Windows endpoints when following conditions are true:



- Windows Firewall is turned off.
- Antivirus (AV) is not running.
- AV signature definitions are not up to date

FortiSASE-Sovereign applies an AND logic for tagging rules under one security posture tag.

Considerations

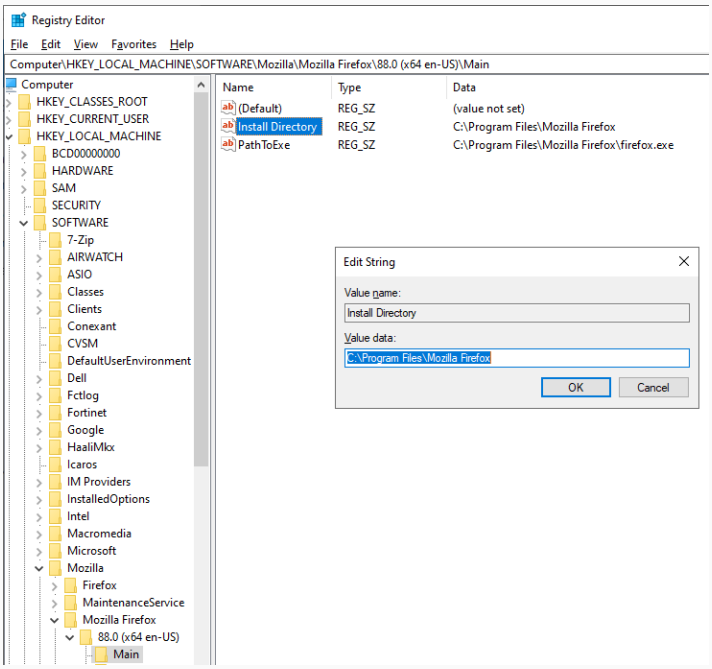
- Using security posture tags for Secure Internet Access policies is recommended to control granular application access based on security posture. With this usage, it is recommended that an allow-all policy remains in place to allow general internet traffic for all users.

Tagging Rule Types

The following table describes tagging rule types and the operating systems (OS) that they are available for. For all rule types, you can configure multiple conditions using the + button.

Rule type	OS	Description
AntiVirus	• Windows • macOS • Linux	From the AntiVirus dropdown list, select the desired conditions. You can require that an endpoint have antivirus (AV) software installed and running and that the AV signature is up-to-date. You can also use the Negate option for the rule to require that the endpoint does not have AV software installed or running or that the AV signature is not up-to-date. This rule applies for FortiClient AV. For Windows endpoints, this rule type also applies for third-party AV software that registers to the Windows Security Center. The third-party software notifies the Windows Security Center of the status of its signatures. FortiClient queries the Windows Security Center to determine what third-party AV software is installed and if the software reports signatures as up-to-date. The endpoint must satisfy all configured conditions to satisfy this rule.
Certificate	• Windows • macOS • Linux	In the Subject CN and Issuer CN fields, enter the certificate subject and issuer. When using FortiClient 7.4, Subject CN supports simple, regular expression, and wildcard matching as selected in the Subject Match dropdown list.
Domain	• Windows • macOS	In the Domain field, enter a domain name. You can use Negate for rules to require that endpoint must not belong to specified domain. Click + to specify additional domains. If you specify multiple domains, FortiSASE-Sovereign considers the endpoint as satisfying the rule if it belongs to any specified domain.

Rule type	OS	Description
EMS Management	• Windows • macOS • Linux • iOS • Android	FortiSASE-Sovereign considers the endpoint as satisfying the rule if the endpoint has FortiClient installed and Telemetry is connected.
File	• Windows • macOS • Linux	In the File field, enter the file path. You can also use Negate to indicate that the rule requires that a certain file is not present on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C.
IP Range	• Windows • macOS • Linux • iOS • Android	In the IP Range field, enter the IP address, IP address range, or IP address with subnet. If multiple IP ranges and/or addresses are configured, FortiSASE-Sovereign considers the endpoint as satisfying the rule if its IP address matches one of the configured ranges or addresses.
Operating System Version	• Windows • macOS • Linux • iOS • Android	From the Operating System Version field, select the OS version. If the rule is configured for multiple OS versions, FortiSASE-Sovereign considers the endpoint as satisfying the rule if it has one of the configured OS versions installed. The following option is available for Windows: • Enable latest update check: FortiSASE-Sovereign checks if Windows OS updates were recently installed.
Registry Key	• Windows	In the Key field, enter the registry path or value name. End the path with \ to indicate a registry path, or without \ to indicate a registry value name. You can also use the Negate option to indicate that the rule requires that a certain registry path or value name is not present on the endpoint. This rule does not support using the value data. For example, the following shows a system where Firefox is installed. In this example, the registry path is HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main. The value name is Install Directory, and the value data is C:\Program Files\Mozilla Firefox. You can configure a registry key rule to match HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\88.0 (x64 en-US)\Main as the path or Install Directory as the registry value name, but you cannot configure a rule to match C:\Program Files\Mozilla Firefox. Do not use square brackets when configuring this rule type.

Rule type	OS	Description
		 The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require registry key A, registry key B, and NOT registry key C, then the endpoint must have both registry keys A and B and not registry key C.
Running Process	• Windows • macOS • Linux	In the Process Name field, enter the process name. You can also use the Negate option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all configured conditions to satisfy this rule. For example, if the rule is configured to require process A, process B, and NOT process C, then the endpoint must have both processes A and B running and process C not running.
Sandbox	• Windows • macOS • Linux	From the Sandbox Detection dropdown list, select the desired condition. You can require that Sandbox detected malware on the endpoint in the last seven days. You can also use the Negate option for the rule to require that Sandbox did not detect malware on the endpoint in the last seven days.
Severity Level	• Windows • macOS • Linux	Specify the desired vulnerability severity range using one or more of the following levels: Any, Medium, High, or Critical. When you select multiple severity levels, FortiSASE-Sovereign considers the endpoint compliant if it has a vulnerability matching any of the selected levels or higher.
User Identity	• Windows • macOS • Linux	Under User Identity, select the following: • User Specified: endpoint user manually entered their personal information in FortiClient.

Rule type	OS	Description

	• iOS
	• Android
		• Social Network Login: endpoint user provided their personal information by logging in to their Google, LinkedIn, or Salesforce account in FortiClient. You can further select one of the following:
		  • All Accounts: all endpoints where the user logged in to the specified social network account type.
		  • Specified: enter a specific Google, LinkedIn, or Salesforce account. For example, you can enter joanexample@gmail.com to configure the rule to apply specifically to only that Google account. You can specify multiple social network accounts.
		FortiSASE-Sovereign considers the endpoint as satisfying the rule if it satisfies one of the conditions.
		You can also use Negate for the rule to require that the endpoint user has not manually entered user details or logged in to a social network account to allow FortiClient to obtain user details.
		FortiClient (iOS) does not support social network login with LinkedIn or Salesforce. FortiClient (Android) does not support social network login with Salesforce.

Windows Security	• Windows	From the Windows Security dropdown list, select the desired conditions. You can require that an endpoint have Windows Defender, BitLocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows Firewall enabled. You can use Negate for the rule to require that the endpoint have Windows Defender, BitLocker Disk Encryption, Exploit Guard, Application Guard, and/or Windows firewall disabled. The endpoint must satisfy all configured conditions to satisfy this rule.
On-Net status	• Windows • macOS • Linux • iOS • Android	You must enable On-net detection and specify an On-net rule set under respective endpoint profiles to tag the endpoint with On-Net status. You can also use the Negate option to indicate that the rule requires that the endpoint is Off-Net.

ZTNA Fabric Device

Syncing ZTNA tags between FortiSASE-Sovereign and the ZTNA application gateway for RBAC

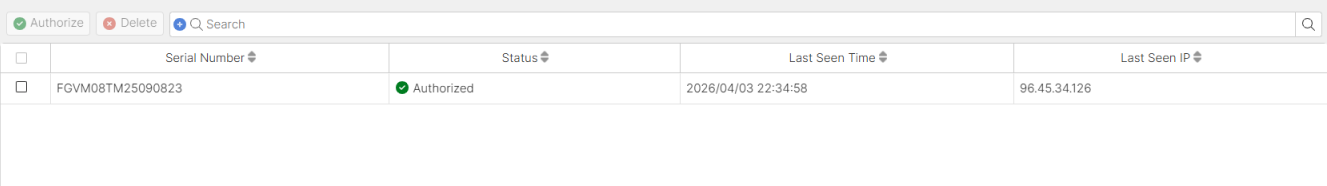
FortiSASE-Sovereign can share configured ZTNA tags with the ZTNA application gateway (i.e. FortiGate) to enforce role-based access control (RBAC) for ZTNA applications. To enable this integration, the FortiGate must

be connected to FortiClient EMS Cloud. See Configuring FortiClient EMS.

You can find EMS Cloud Domain in System > Service Settings > EMS Configuration > EMS Domain for Fabric Connector.

Once the FortiGate is connected to FortiClient Cloud, you can deny or authorize the ZTNA application gateway. Only authorized FortiGates can synchronize endpoint and tagging data from FortiSASE-Sovereign for access control enforcement.

To authorize or delete the ZTNA application gateway on FortiSASE-Sovereign:



1. Go to Endpoint Management > ZTNA Fabric Device.
2. Click Authorize or Delete. The FortiGate status changes.

Considerations

- If a FortiGate ZTNA application gateway is running FortiOS 7.4.4 or later, then FortiSASE-Sovereign automatically learns TCP forwarding and non-Web ZTNA applications previously configured on the FortiGate.

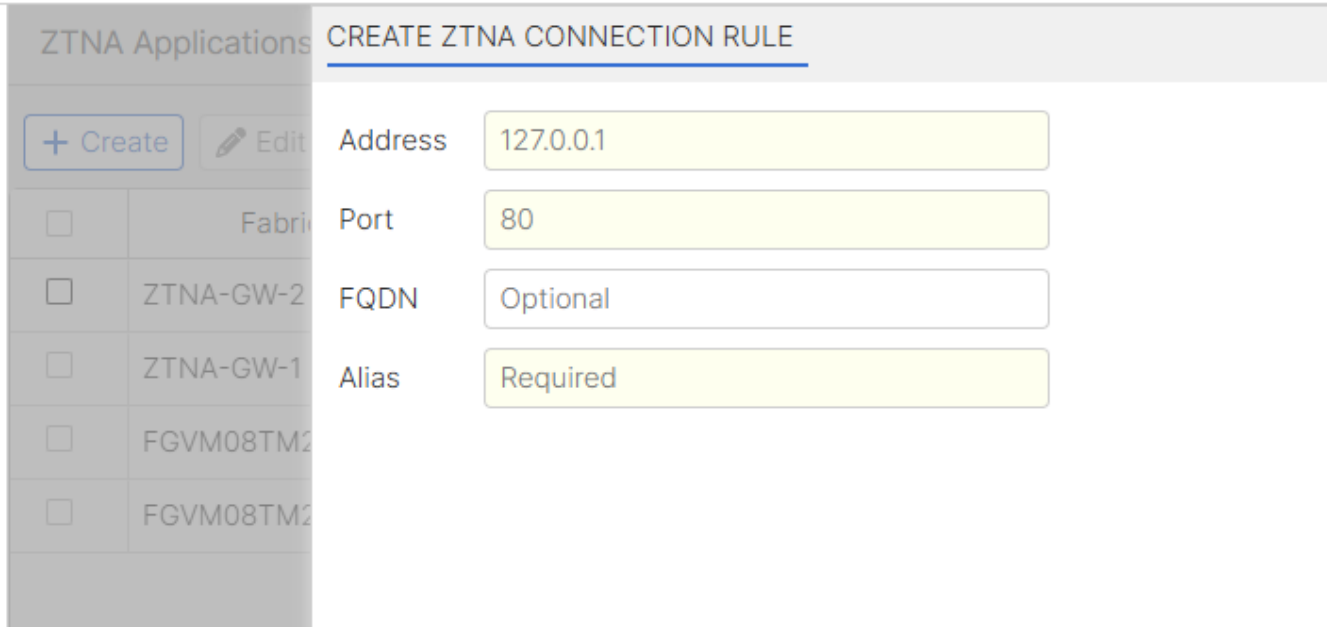
ZTNA Application Catalogue

Zero trust network access (ZTNA) application gateways and applications are key components in the FortiSASE-Sovereign ZTNA solution for agent-based remote users. A ZTNA application gateway serves as a secure entry point that mediates the connection between remote users and internal ZTNA applications. A ZTNA application represents the actual application or service that remote users attempt to access. A ZTNA application can be any internal web or enterprise application, cloud service, or on-premise resource. A ZTNA application gateway acts as a reverse proxy, ensuring that only authorized and compliant users can access ZTNA applications based on security policies that the organization defines. You can configure a FortiGate to serve as the ZTNA application gateway. See Zero Trust Network Access.

FortiSASE-Sovereign enables administrators to configure and manage ZTNA application gateways and ZTNA application configurations for agent-based remote users in Endpoint Management > ZTNA Application Catalogue.

Once you configure ZTNA application gateways and applications, you can reference and use them in individual endpoint profiles on the ZTNA tab.

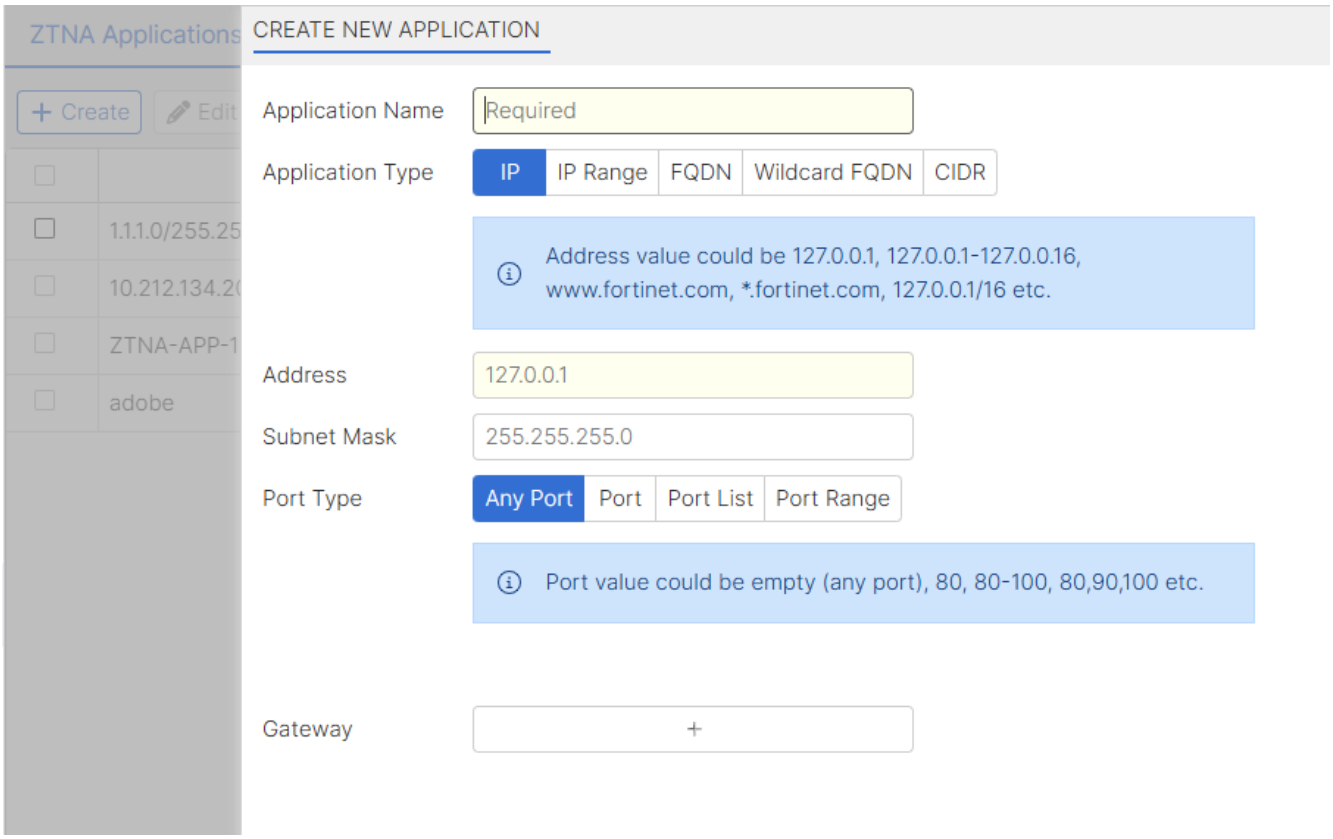
To configure ZTNA application gateway on FortiSASE-Sovereign:



1. Go to Endpoint Management > ZTNA Application Catalogue.
2. Select the ZTNA Gateways Catalogue tab.
3. Click Create and enter the following details for the ZTNA application gateway:

Field	Value
Address	Specify IP address of the FortiGate that is configured to act as the ZTNA application gateway.
Port	Specify port number on FortiGate that is designated for ZTNA access.
FQDN	Optionally, specify the FQDN of the FortiGate that is configured to act as the ZTNA application gateway.
Alias	Enter a unique name for your application gateway.

To configure ZTNA application on FortiSASE-Sovereign:



1. Go to Endpoint Management > ZTNA Application Catalogue.
2. Select ZTNA Applications Catalogue tab.
3. Click Create to configure new ZTNA application, and enter the following details:

Field	Value
Application Name	Enter unique name for your application.
Application Type	Select either from IP, IP Range, FQDN, Wildcard FQDN or CIDR.
Address & Subnet Mask	Based on Type selected, specify either IP address with subnet mask or FQDN of the ZTNA application.
Port Type & Port	Select Any or Port, Port List, Port Range to enter a specific port number or port set.
Gateway	Click + to select Application gateway configured in earlier steps.

4. Click OK.

ZTNA gateways and ZTNA applications created using above steps are determined as manual ZTNA gateways and applications. Such gateways and applications can be edited or deleted later. If you authorized remote FortiGate ZTNA gateways through ZTNA Fabric Device, FortiSASE-Sovereign will also sync ZTNA gateways and applications previously configured on remote FortiGate ZTNA gateways, and these ZTNA gateways and

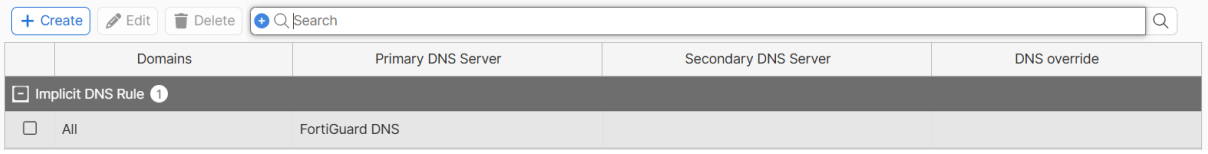
applications are determined as auto-detected. You cannot edit or delete auto-detected ZTNA gateways and applications. They can be removed by delete the remote ZTNA gateways from ZTNA Fabric Device.

DNS

Remote users use the DNS server in FortiSASE-Sovereign under Endpoint Management > DNS to resolve hostnames for internal and external domains.

Agent and agentless endpoints and endpoints connected to authorized Edge devices forward their DNS traffic to FortiSASE-Sovereign PoP FortiGates. FortiSASE-Sovereign performs transparent DNS redirection to redirect DNS traffic conditionally as desired.

- Implicit DNS rules are predefined for agents and users connected to authorized Edge devices. FortiSASE-Sovereign uses these rules for resolving hostnames for external domains.
- You can create split DNS or DNS redirection rules by clicking Create. FortiSASE uses these rules for resolving hostnames for internal domains.



By default, FortiSASE-Sovereign deployments use FortiGuard DNS as the default DNS server for the All implicit DNS rule. You can select any implicit DNS rule and click Edit to change the default DNS server.

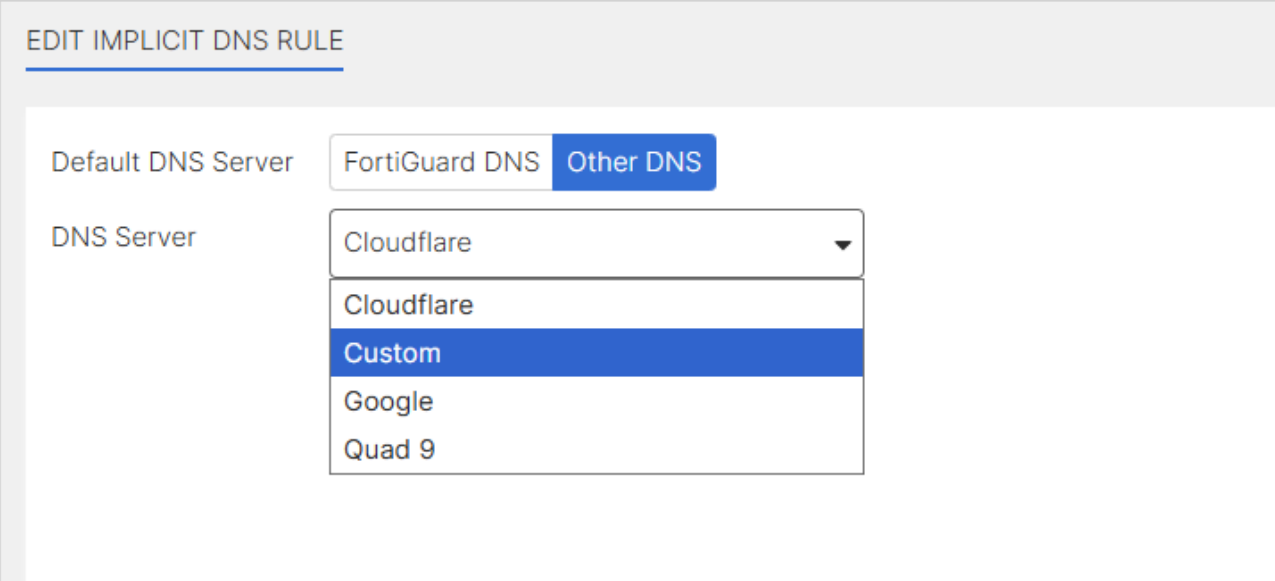
You can configure Default DNS Server with one of the following options, then click OK to save the change:

DNS Server	Description	Primary and Secondary DNS Server IP Address
FortiGuard DNS	Use FortiGuard DNS.	96.45.45.45 96.45.46.46
Other DNS	Use a public DNS server other than FortiGuard DNS.	IP addresses specific to public DNS server
CloudFlare	Use the CloudFlare public DNS server.	1.1.1.1 1.0.0.1
Custom	Enable to specify your own custom primary and secondary DNS servers.	Specify IP address of primary and secondary DNS.
Google	Use the Google public DNS server.	8.8.8.8 8.8.4.4
Quad 9	Use the Quad 9 public DNS server.	9.9.9.9 149.112.112.112

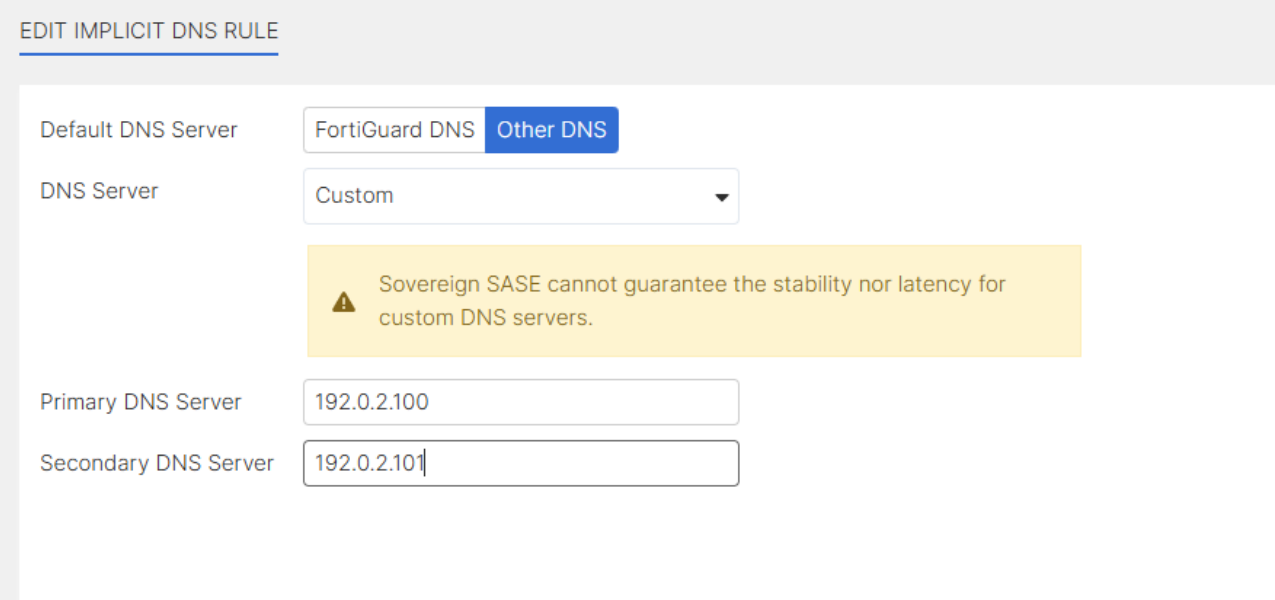
For example, you can edit the implicit DNS rule to use a custom DNS server as follows:

To configure a custom DNS server:

1. Go to Endpoint Management > DNS, select the All implicit DNS rule, and click Edit.
2. In the Edit Implicit DNS Rule page, for Default DNS Server, select Other DNS.
3. From the DNS Server dropdown, select Custom.



4. In the Primary DNS Server and Secondary DNS Server fields, enter the respective IP addresses for the servers of your choice.The screenshot uses IP addresses for documentation and should not be used in a production environment.



5. Click OK.
   Using FortiGuard DNS or another public DNS service is sufficient for most secure internet access (SIA) use cases that simply require remote users to resolve hostnames for external domains.

Considerations

- FortiGuard DNS servers do not support DNS over TCP. If you require DNS over TCP, edit implicit DNS rules from the default FortiGuard DNS server to other DNS servers that support DNS over TCP.
- FortiSASE-Sovereign cannot guarantee the stability nor latency for custom DNS servers. These factors must be considered by the customer or provider maintaining the custom DNS servers.

DNS Redirection Rules

FortiSASE-Sovereign users often must resolve internal hostnames that public DNS servers cannot resolve in scenarios where agent-based users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server. You can configure FortiSASE-Sovereign DNS settings for DNS redirection using DNS redirection rules.

DNS redirection works as follows:

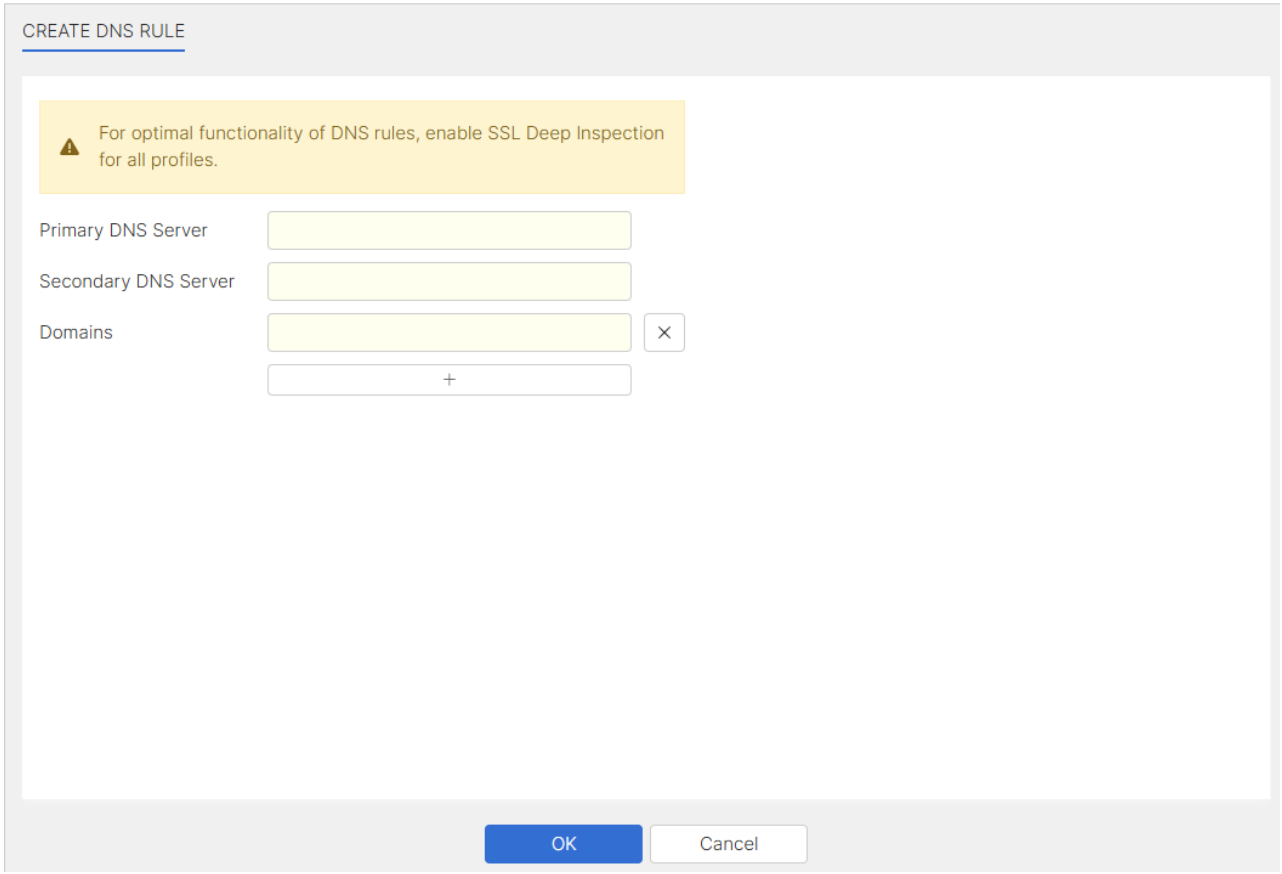
- Agent and agentless endpoints and endpoints connected to authorized edge devices forward all their DNS traffic to FortiSASE-Sovereign PoP FortiGates.
- FortiSASE-Sovereign performs transparent DNS redirection to redirect DNS traffic conditionally as desired.
- Resolve all other hostnames for external domains using the implicit DNS rule.

DNS redirection is more efficient than sending all DNS requests to DNS servers defined in the implicit DNS rules because it reduces any potential latency and downtime with using these DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource DNS server deployments.

Configuring DNS redirection rules

To configure DNS redirection rules:

1. Go to Endpoint Management > DNS.
2. Click Create.



3. In the Create DNS Rule pane, do the following:
   a. Enter the Primary DNS Server, Secondary DNS Server, and one Domains.
   b. (Optional) Click + to add more fields to enter in additional domains.
   c. Click OK to save the DNS redirection rule.
4. The DNS redirection rule has been created and displays in the table.

Considerations

- DNS redirection requires endpoint users are managed by proxy-based security policies and security profiles. Flow-based users will always use system DNS server for DNS resolution.

www.fortinet.com