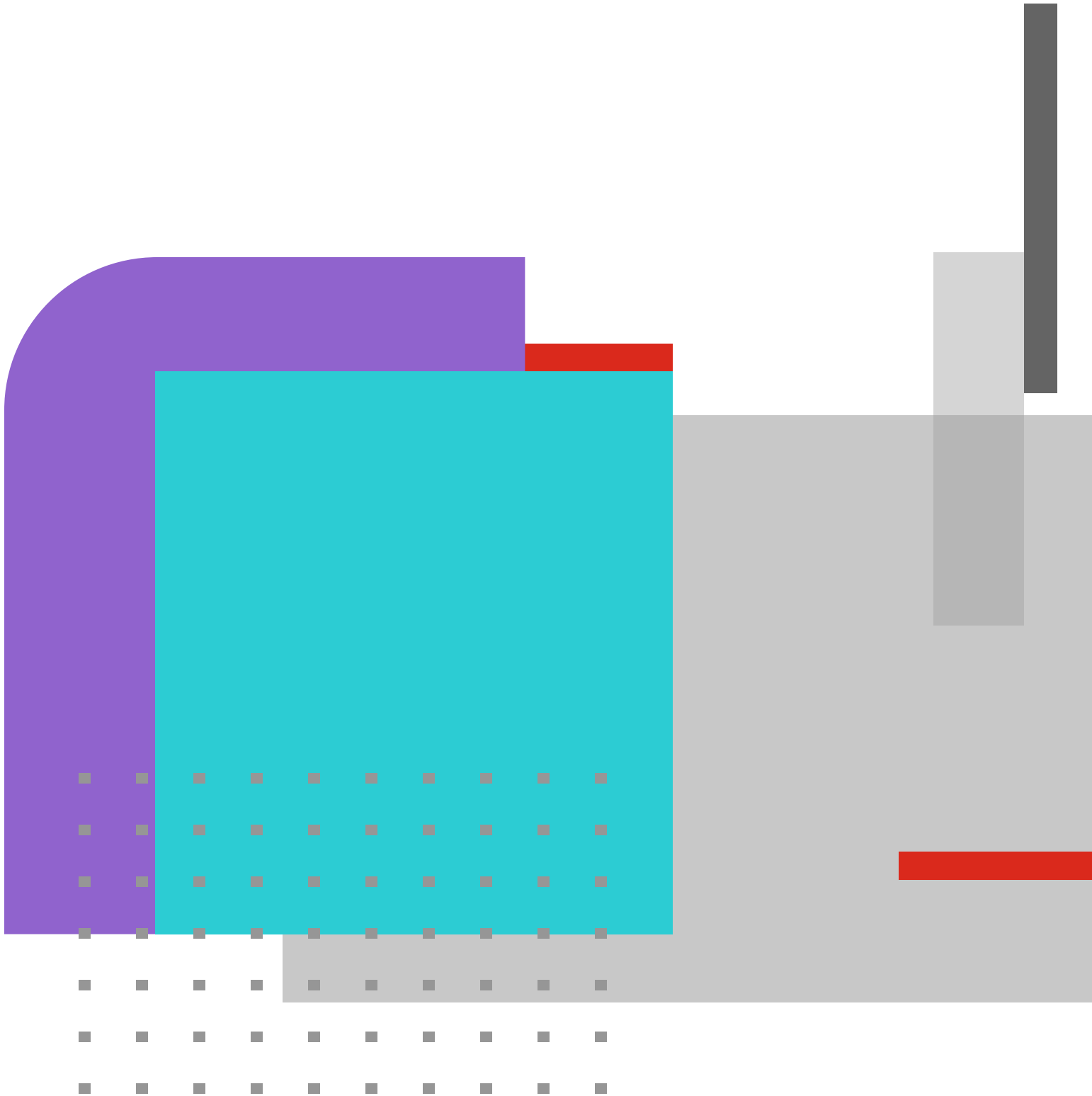


DEPLOYMENT GUIDE

# Veriti Integration



# Table of Contents

About Veriti . . . . .	3
Deployment Prerequisite . . . . .	3
Version Compatibility . . . . .	3
Configuration. . . . .	3
FortiManager Configuration. . . . .	4
Standalone FortiGate Configuration . . . . .	7
Standalone FortiAnalyzer Configuration. . . . .	9
Veriti Configuration. . . . .	11
Integrating with FortiManager. . . . .	11
Integrating with Standalone FortiGate NGFW . . . . .	13
Integrating with Standalone FortiAnalyzer . . . . .	15
Known Limitations. . . . .	17



## About Veriti

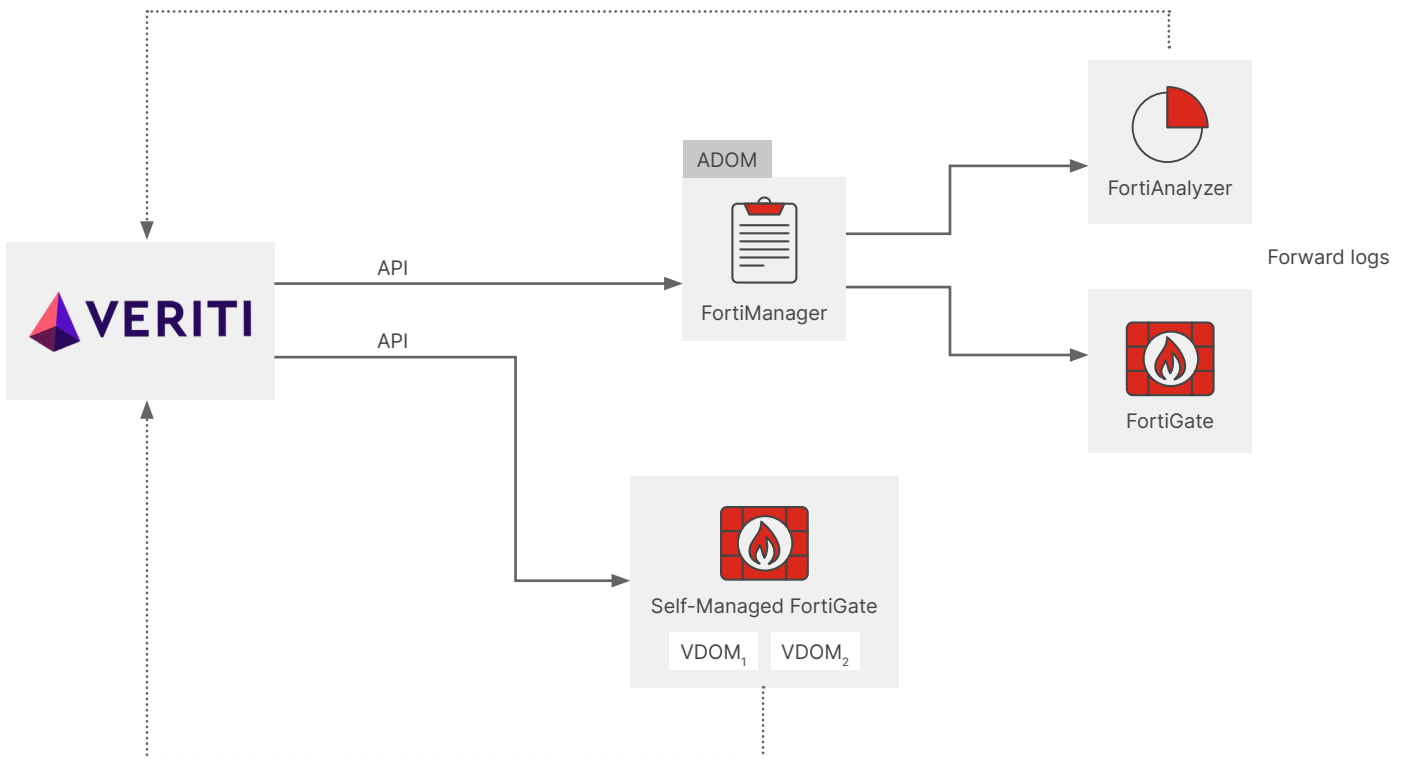
Veriti is a fast-growing cybersecurity innovator that helps organizations maximize their security posture while ensuring business uptime. With Veriti, organizations can eliminate complexity and operational friction in managing multiple cybersecurity solutions with a consolidated, governing platform that proactively monitors and, in a single click, remediates security gaps and misconfigurations across the entire security infrastructure.

## Version Compatibility

This deployment and integration guide applies to FortiManager, FortiGate, and FortiAnalyzer with FortiOS v6.4 or newer.

### Deployment Prerequisite

- FortiGate
- FortiManager (Optional)
- FortiAnalyzer (Optional)
- Veriti Server with network access to Fortinet devices



## Configuration

- Fortinet configuration

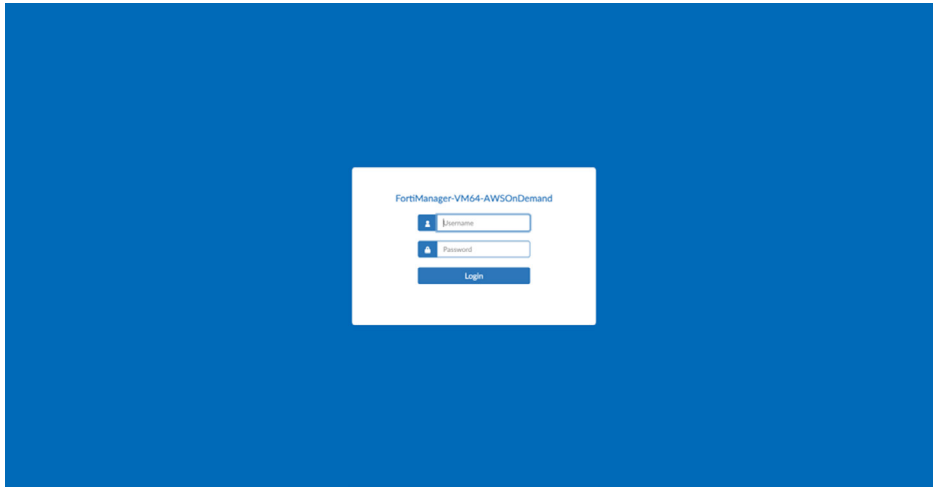
Veriti supports the following Fortinet deployments:

- Fully managed architecture with FortiManager, FortiGate, and FortiAnalyzer
- Managed architecture with FortiManager and FortiGate and standalone FortiAnalyzer
- Managed architecture with FortiManager and FortiGates
- Standalone FortiGate and standalone FortiAnalyzer
- Standalone FortiGate

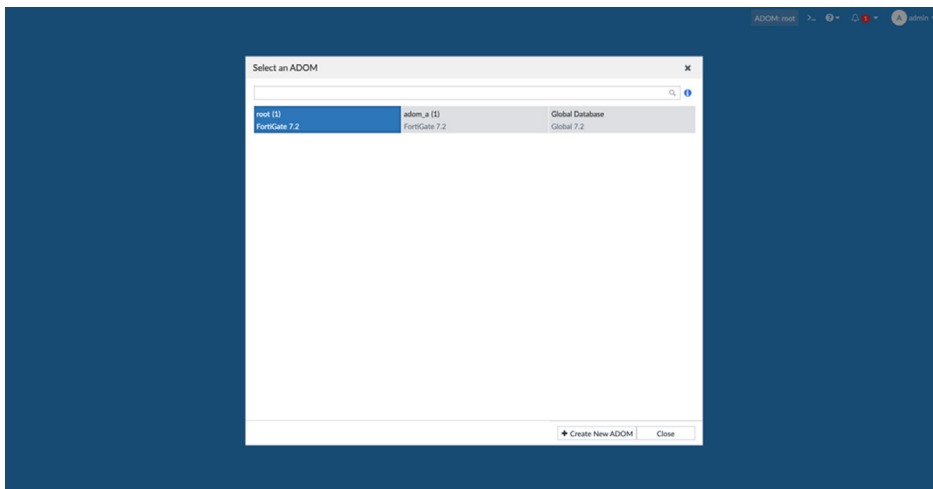
Configure a new user with the required permissions to initiate communication between Veriti and Fortinet devices, along with the remote utilization of API commands.

**FortiManager Configuration:**

1. Log in to FortiManager GUI.



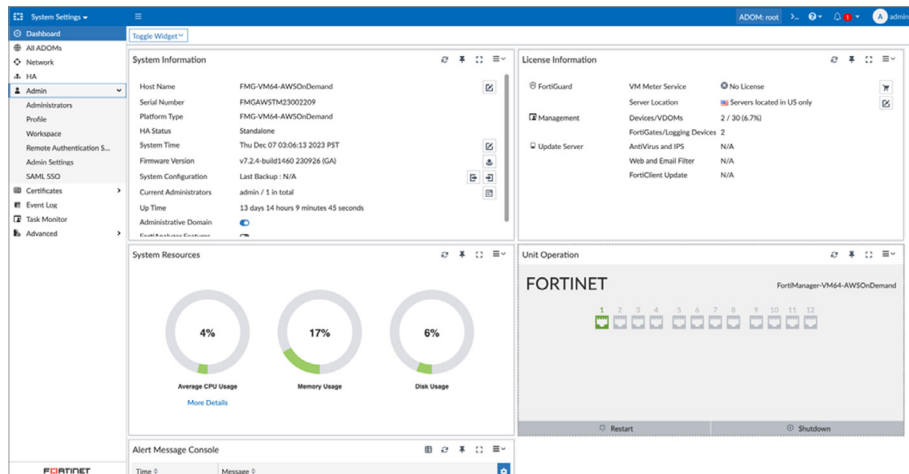
2. Select an ADOM (if the ADOM feature is enabled).



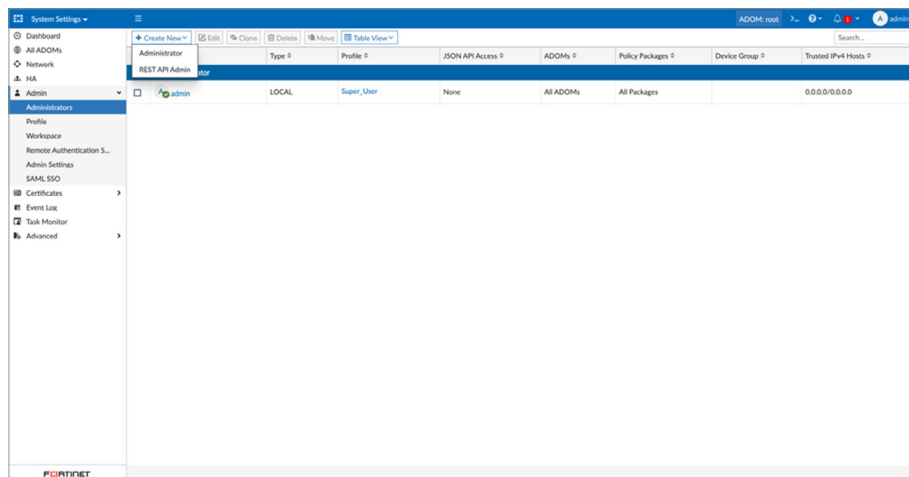
3. Click on "System Settings."



4. On the left panel, click on “Administrators.”



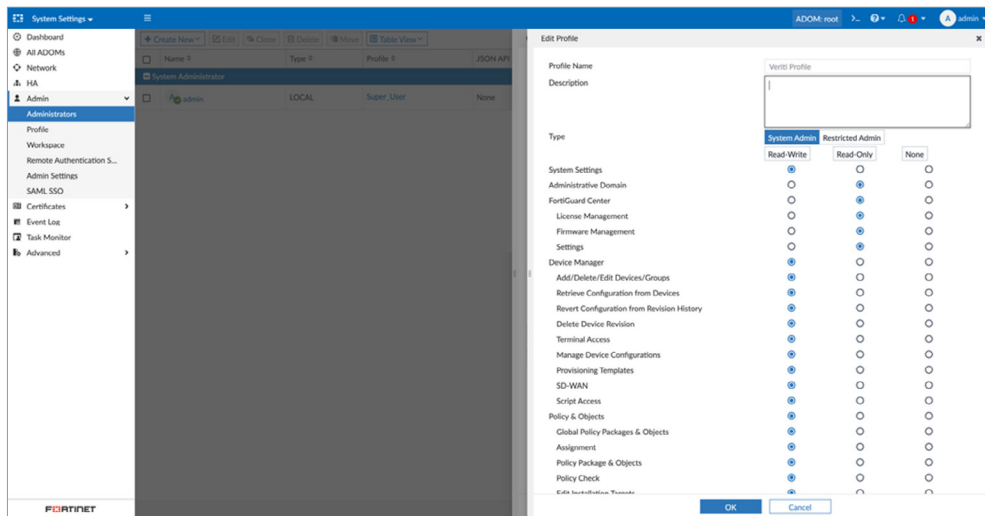
5. Click “Create New” at the top toolbar and choose “Administrator.”



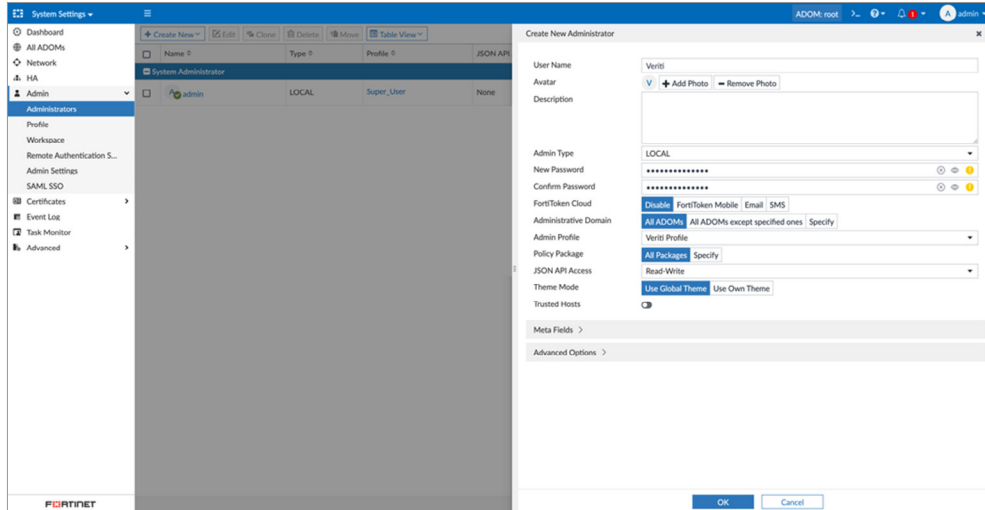
6. Fill the following details in the “Create New Administrator” menu:

- Username
- Admin Type (make sure it is “LOCAL”)
- New Password
- Confirm Password
- Administrative Domain (make sure it is “All ADOMs” if the ADOM feature is enabled)
- Admin Profile – create a new profile by clicking on “+” with the following data:
  - Profile Name
  - Type (make sure it is “System Admin”)
  - Read-Write permissions:
    - System Settings
    - Device Manager (and its sub permissions)
    - Policy & Objects (and its sub permissions) – required only if remediations will be taken from Veriti
    - Install Policy Package or Device Configuration – required only if remediations will be taken from Veriti
  - Read-Only permissions (all other permissions)



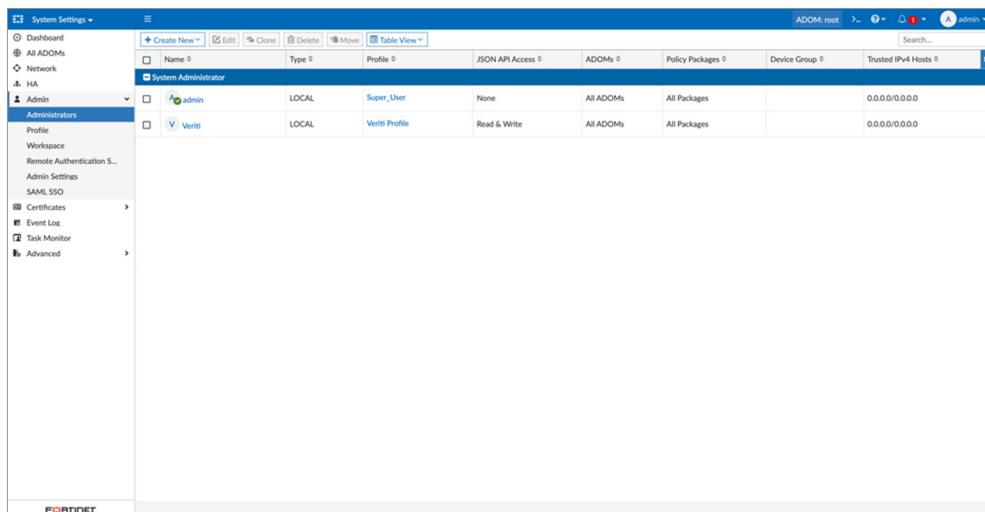


g. JSON API Access (make sure it is “Read-Write”).



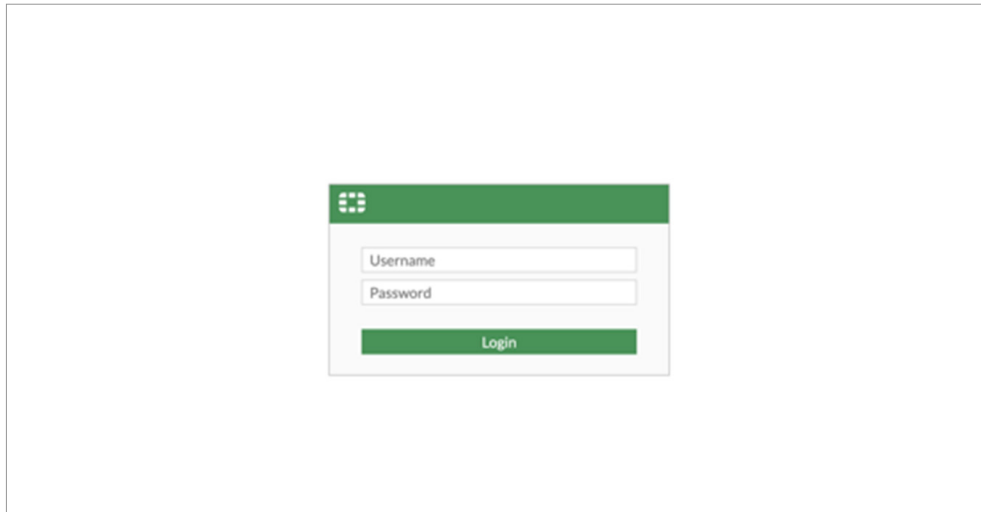
7. Click “OK.”

8. Verify the new user is presented in the “System Administrators” table.

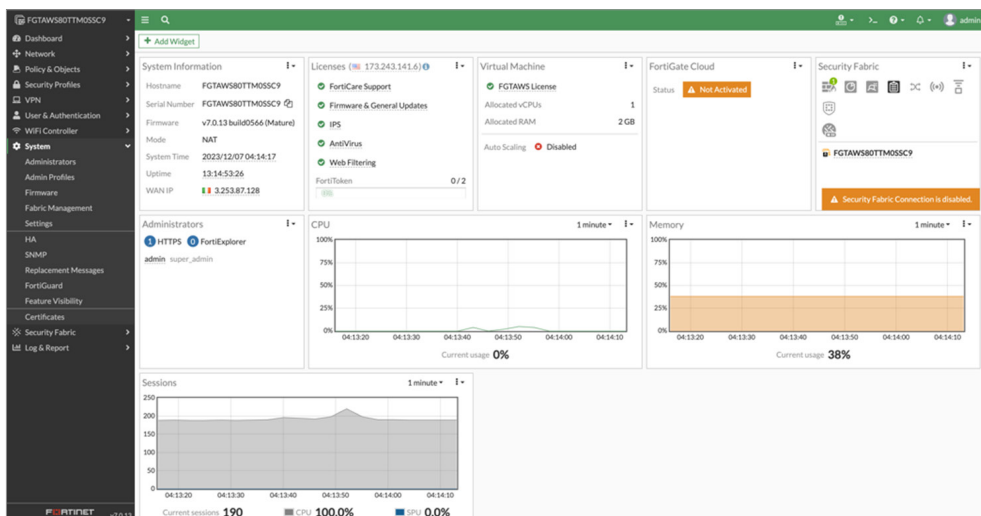


## Standalone FortiGate Configuration:

1. Log in to FortiGate GUI.



2. On the left panel, click "System" and choose "Administrators."

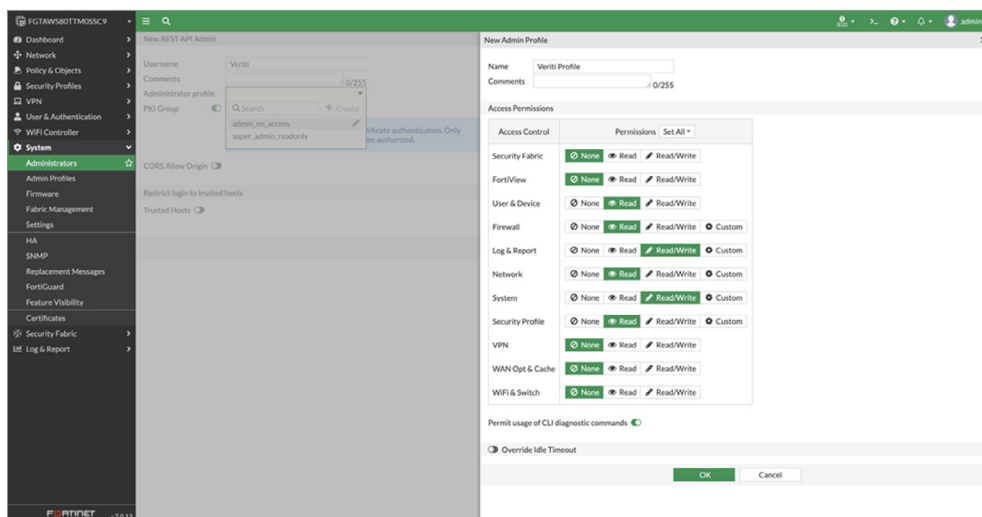


3. Click "Create New" at the top toolbar and choose "REST API Admin."

Administrator	Type	Profile	JSON API Access	ADOMs	Trusted IPv4 Hosts
REST API Admin	user				
admin	LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0

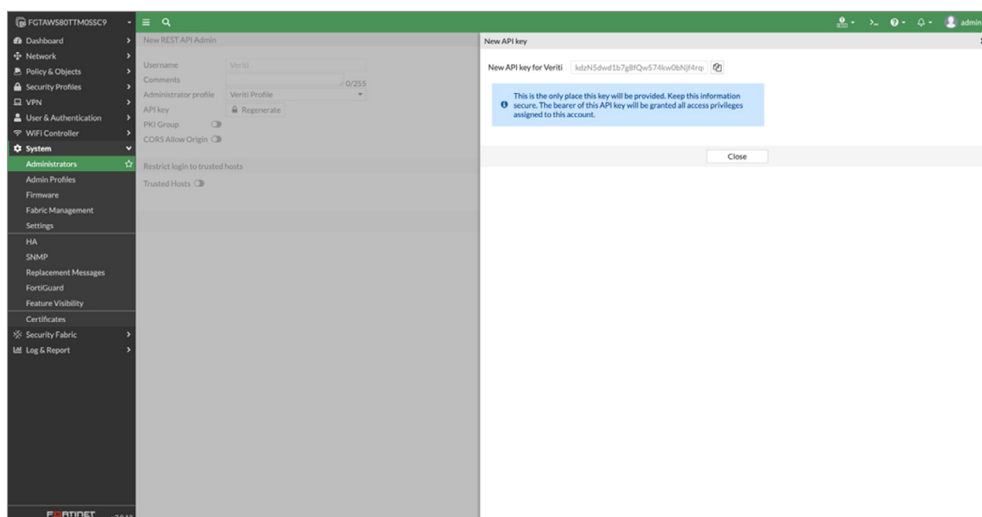
4. Fill in the following details on the “New REST API Admin” page:

- a. Username
- b. Administrator Profile – create a new profile by clicking on “+ Create” with the following data:
  - i. Name
  - ii. Read/Write permissions:
    1. Log & Report
    2. System
    3. Security Profiles are required only if remediations are taken from Veriti; otherwise, they should be “Read”
  - iii. Read permissions:
    1. User & Device
    2. Firewall
    3. Network
  - iv. None Permissions (all other permissions)



5. Click “OK.”

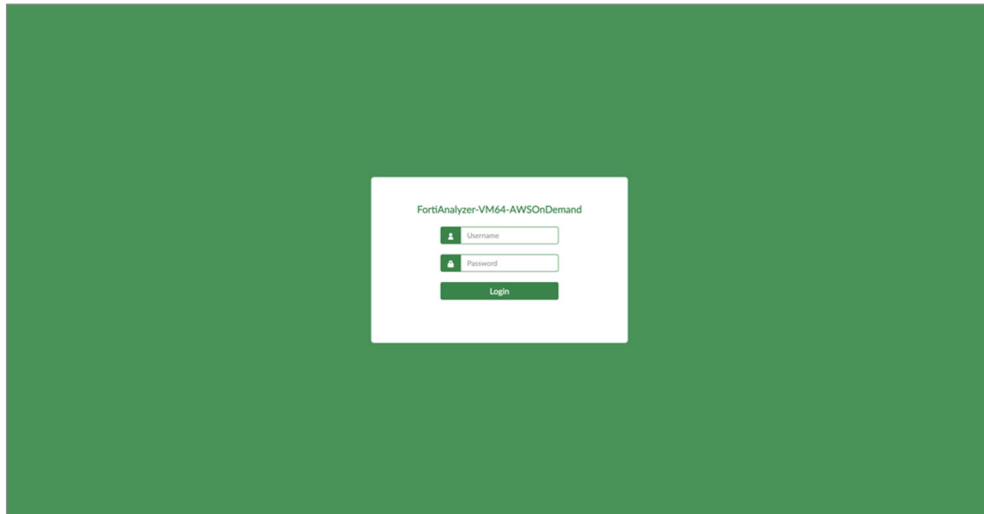
6. Copy the generated “API Key” and store it for later use.



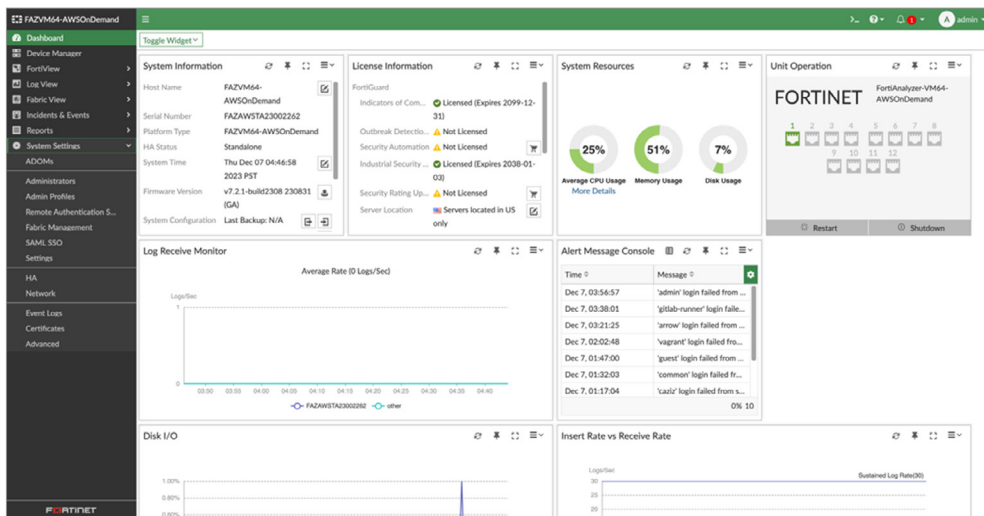


## Standalone FortiAnalyzer Configuration:

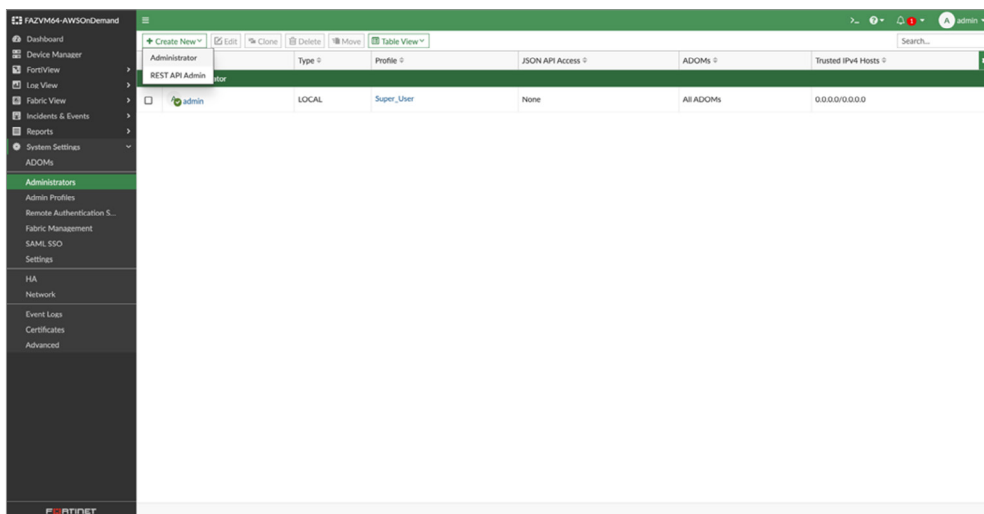
1. Log in to FortiAnalyzer GUI.



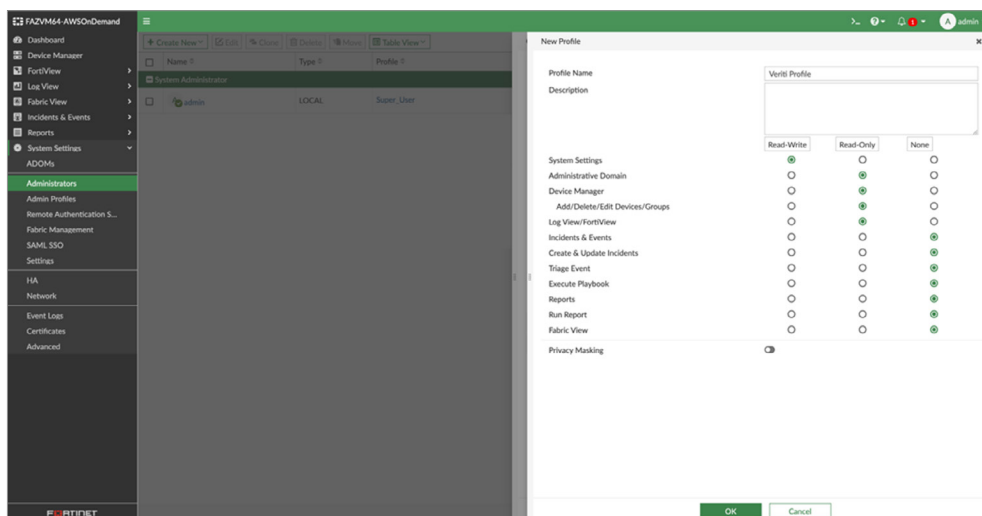
2. Click "System Settings" on the left panel and choose "Administrators."



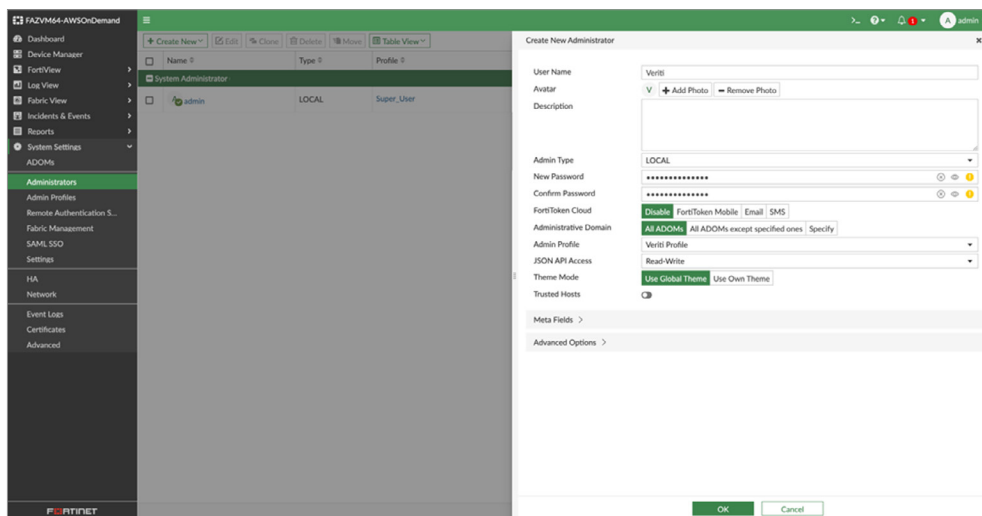
3. Click "Create New" at the top left toolbar and choose "Administrator."



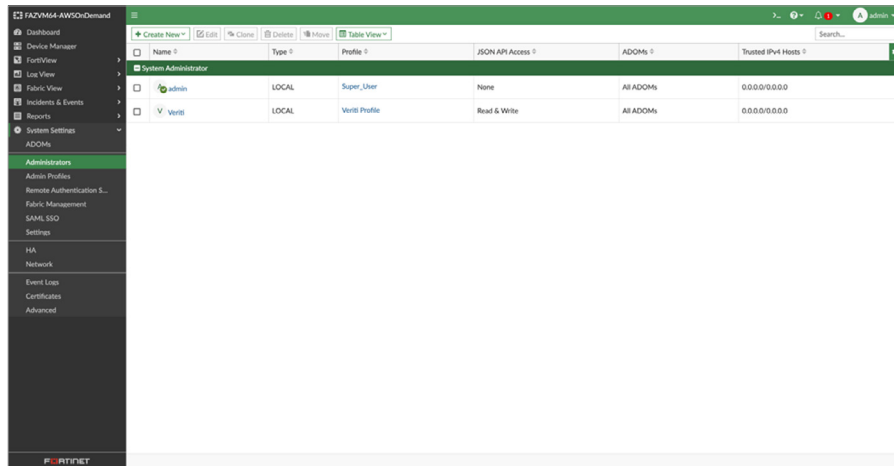
4. Fill the following details in the “Create New Administrator” menu:
  - a. Username
  - b. Admin Type (make sure it is “LOCAL”)
  - c. New Password
  - d. Confirm Password
  - e. Administrative Domain (make sure it is “All ADOMs” if the ADOM feature is enabled)
  - f. Admin Profile – create a new profile by clicking on “+” with the following:
    - i. Profile Name
    - ii. Read-Write permissions:
      1. System Settings
    - iii. Read-Only permissions:
      1. Administrative Domain
      2. Device Manager (and its sub permissions)
      3. LogView/FortiView
    - iv. None Permissions (all other permission)



5. Click “OK.”



6. Verify the new user is presented in the “System Administrators” table.



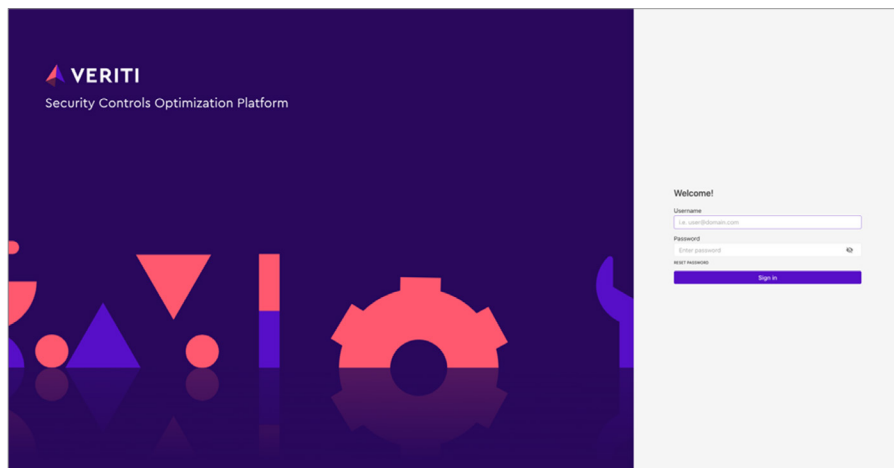
Name	Type	Profile	JSON API Access	ADOMs	Trusted IPv4 Hosts
admins	LOCAL	Super User	None	All ADOMs	0.0.0.0/0.0.0.0
Veriti	LOCAL	Veriti Profile	Read & Write	All ADOMs	0.0.0.0/0.0.0.0

## Veriti Configuration

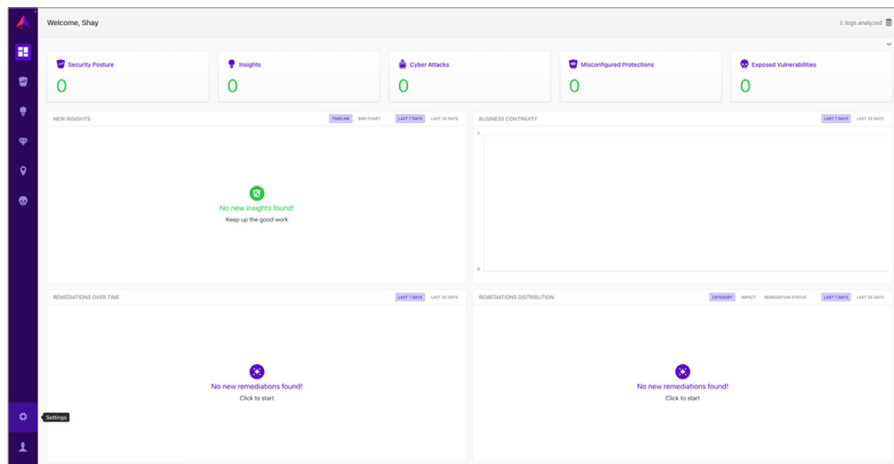
The Veriti platform requires that you initialize connections with the relevant device to fetch the relevant data from your security products.

### Integrating with FortiManager:

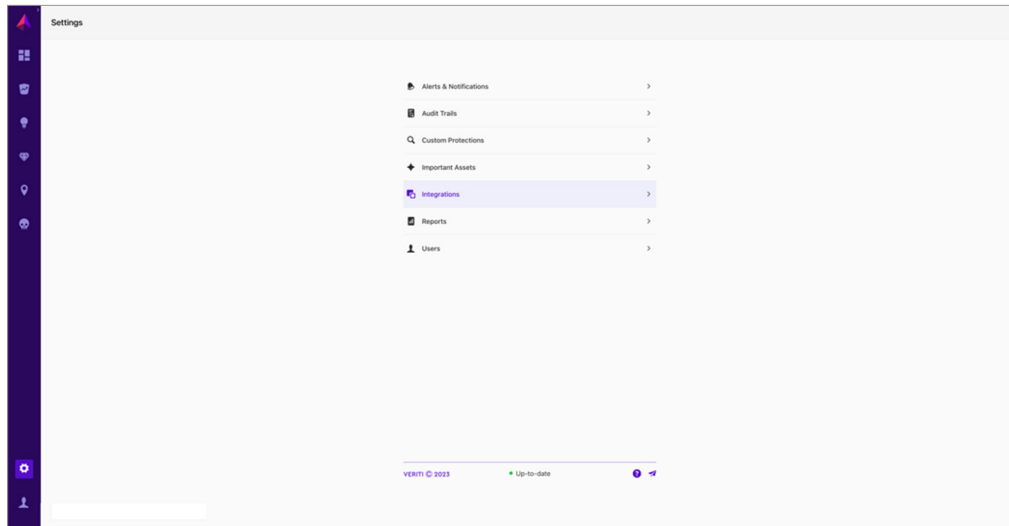
1. Log in to Veriti Portal via [https://<veriti\\_server\\_ip>:30002](https://<veriti_server_ip>:30002) and enter your credentials.



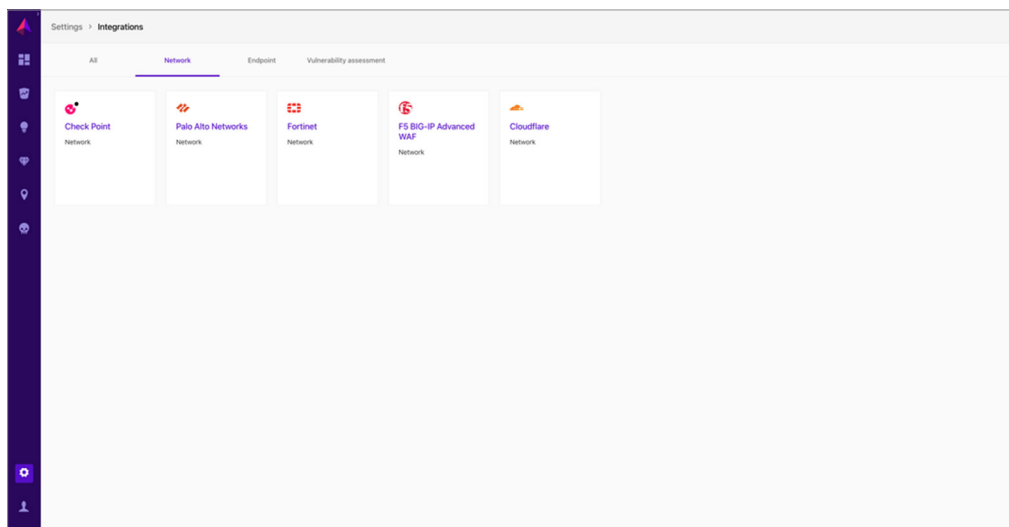
2. On the left panel, click on “Settings.”



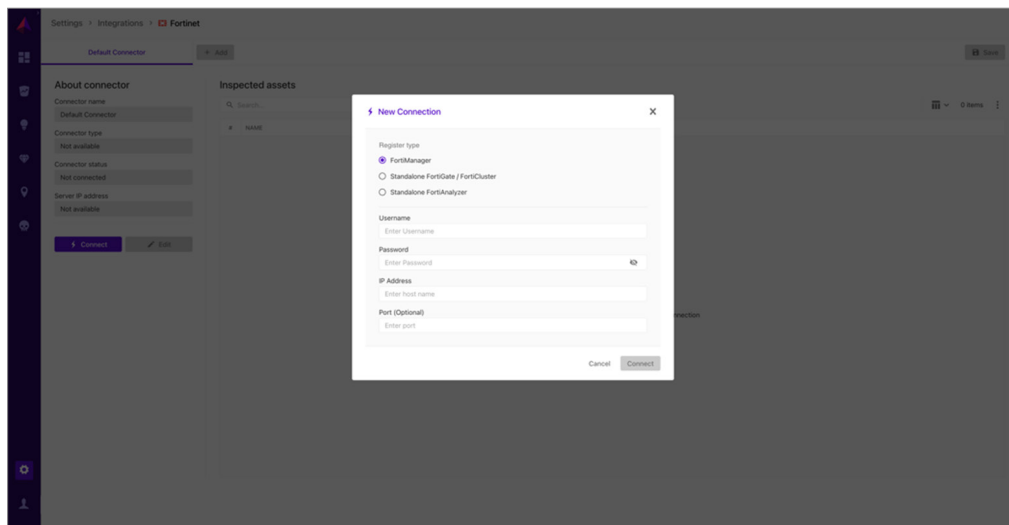
3. Click on "Integrations."



4. On the top panel, click "Network" and choose "Fortinet."



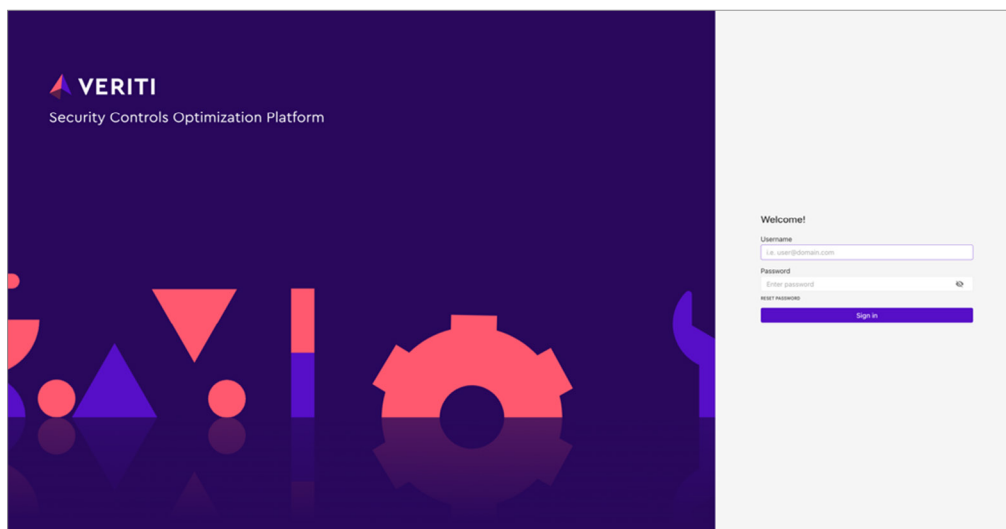
5. On the connector page, click "Connect" and choose "FortiManager" as the registration type.



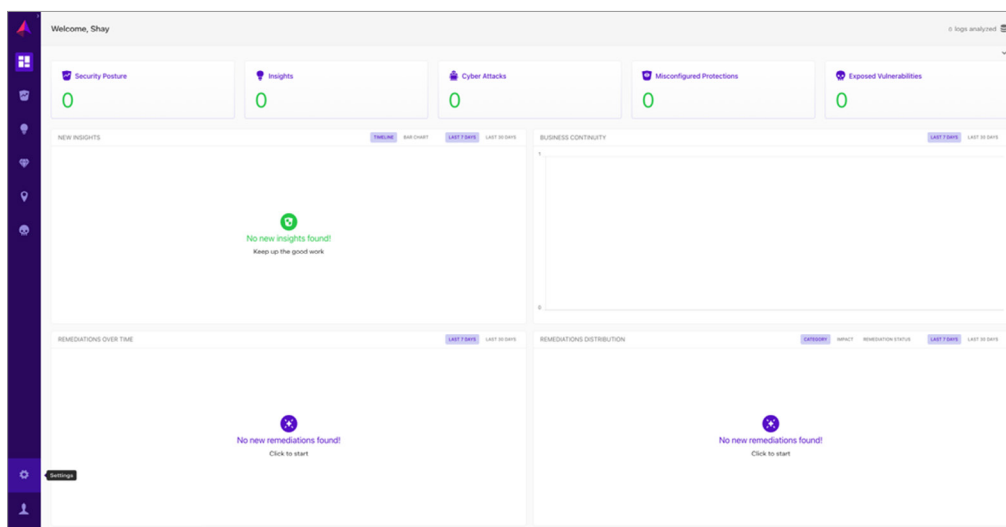
6. Fill in the following details in the “New Connection” menu:
  - a. Username
  - b. Password
  - c. FortiManager IP Address
  - d. Port (optional – by default, it is 443)
7. Click “Connect.”
8. Verify your FortiManager and managed devices are presented in the “Inspected Assets” table.
9. Click “Save” on the top right to start fetching data from your devices.

### Integrating with Standalone FortiGate NGFW:

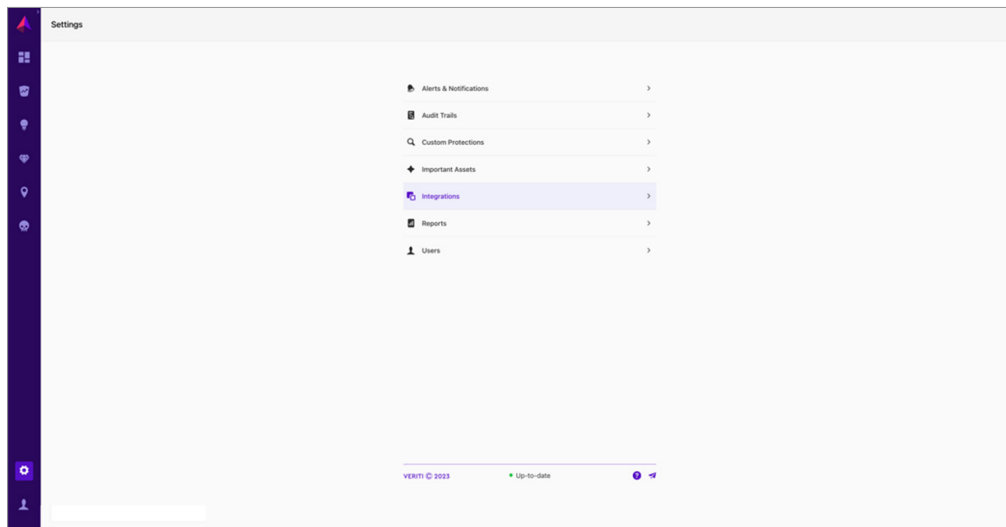
1. Log in to Veriti Portal via [https://<veriti\\_server\\_ip>:30002](https://<veriti_server_ip>:30002) and enter your credentials.



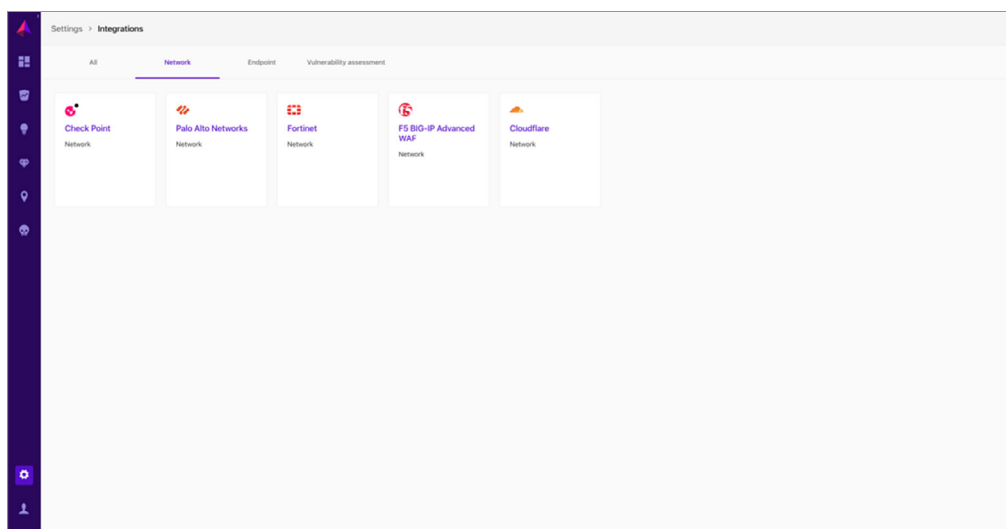
2. On the left panel, click on “Settings.”



3. Click on “Integrations.”



4. On the top panel, click “Network” and choose “Fortinet.”



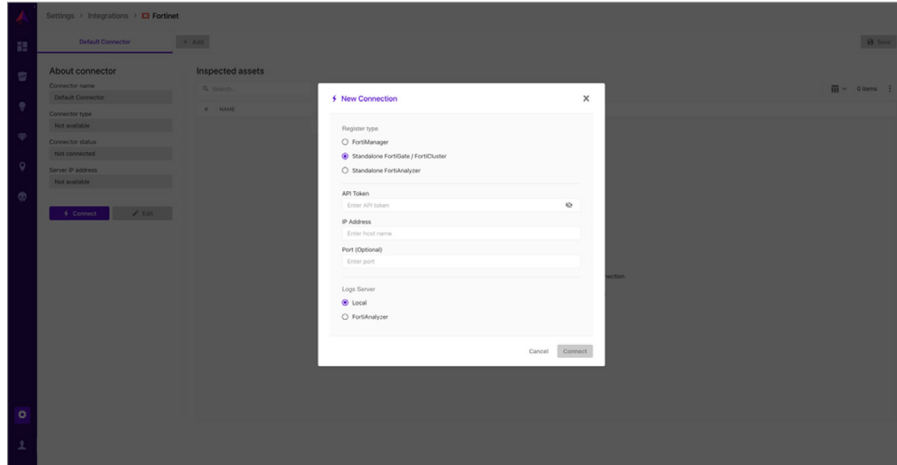
5. On the connector page, click “Connect” and choose “Standalone FortiGate” as the registration type.

Note: If multiple standalone devices exist, each one will require a new connector.

6. Fill in the following details in the “New Connection” menu:

- a. API Token
- b. FortiGate IP Address
- c. Port (optional – by default, it is 443)
- d. Choose the type of the Log Server:
  - i. Local – If security logs are saved on FortiGate
  - ii. FortiAnalyzer – If security logs are sent and saved on FortiAnalyzer, fill in the following details of the FortiAnalyzer:
    1. Username
    2. Password
    3. FortiAnalyzer IP Address
    4. Port (optional – by default, it is 443)

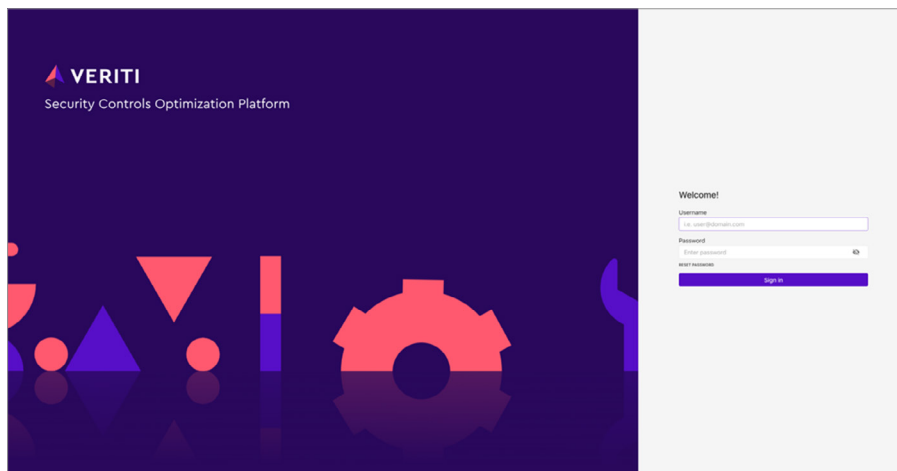




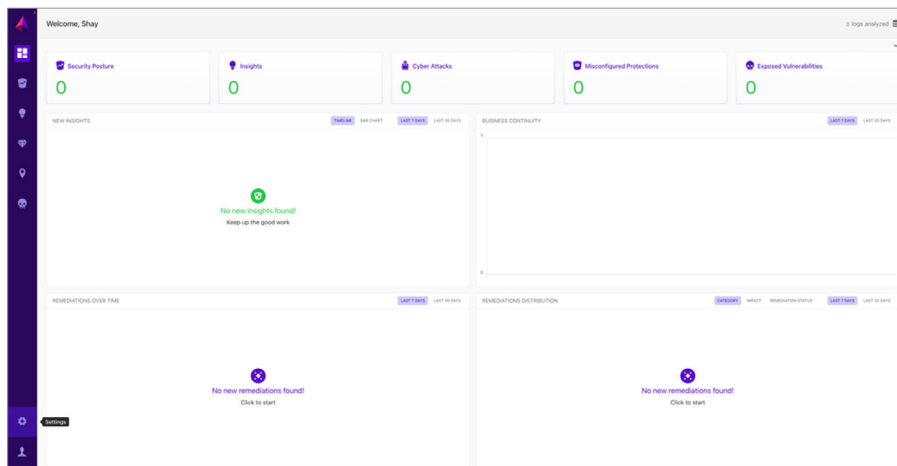
7. Click “Connect.”
8. Verify your FortiGate or FortiAnalyzer is presented in the “Inspected Assets” table.
9. Click “Save” on the top right to start fetching data from your devices.

### Integrating with Standalone FortiAnalyzer:

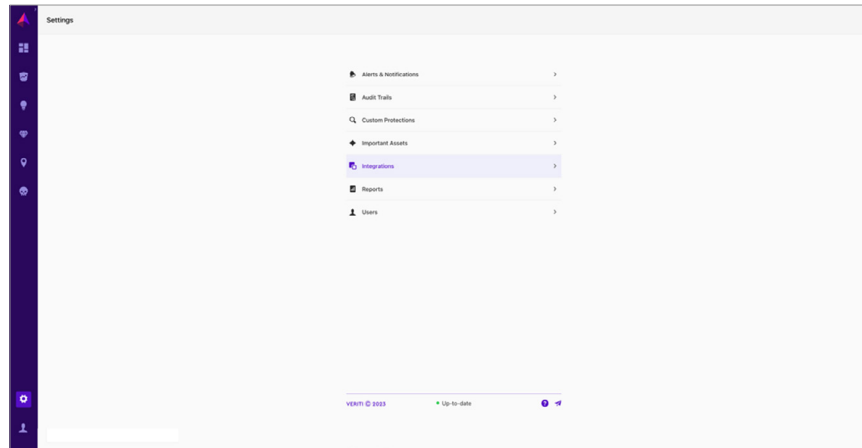
1. Log in to Veriti Portal via [https://<veriti\\_server\\_ip>:30002](https://<veriti_server_ip>:30002) and enter your credentials.



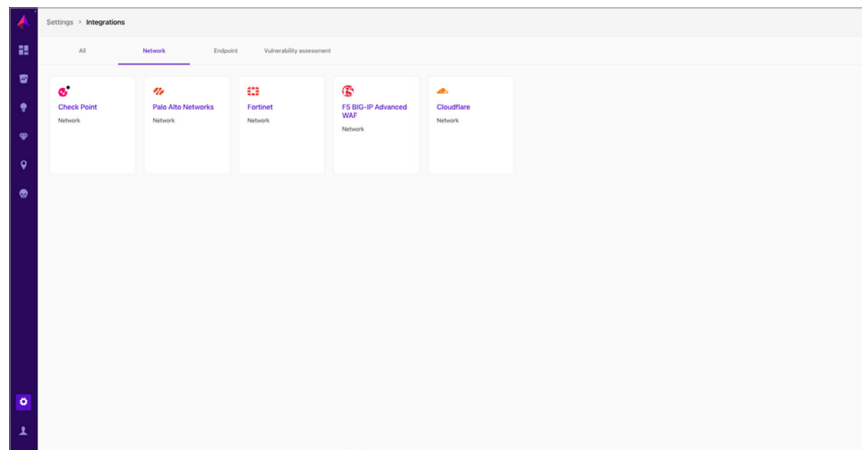
2. On the left panel, click on “Settings.”



3. Click on “Integrations.”



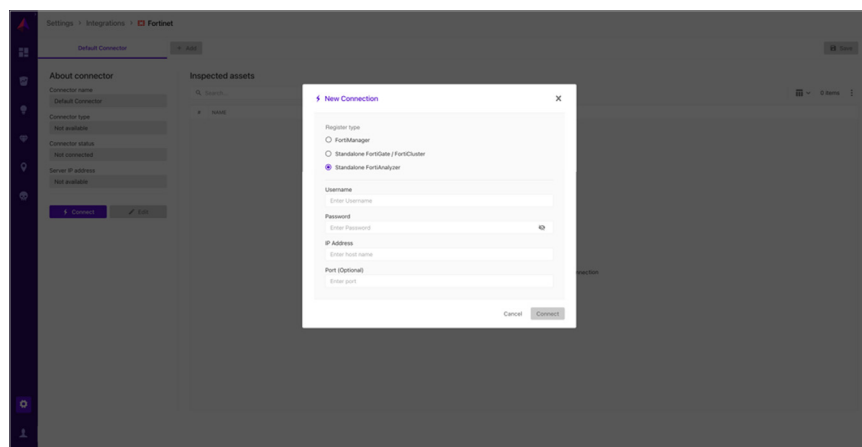
4. On the top panel, click “Network” and choose “Fortinet.”



5. On the connector page, click “Connect” and choose “Standalone FortiAnalyzer” as the registration type.

6. Fill in the following details in the “New Connection” menu:

- a. Username
- b. Password
- c. FortiAnalyzer IP Address
- d. Port (optional – by default, it is 443)





7. Click “Connect.”
8. Verify your FortiAnalyzer is presented in the “Inspected Assets” table.
9. Click “Save” on the top right to start fetching data from your device.

## Known Limitations

- In the absence of FortiManager, remediation of global VDOMs is not supported.
- ADOMs in FortiAnalyzer are currently not supported.



[www.fortinet.com](http://www.fortinet.com)