FORTINET | ziften

DEPLOYMENT GUIDE

Fortinet FortiSandbox and Ziften Zenith

Fortinet FortiSandbox and Ziften Zenith

Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Ziften delivers all-the-time visibility and control for any asset, anywhere—client devices, servers, and cloud VMs—whether on-network or remote; connected or not. Ziften's unified systems management and security platform empowers IT operations and security teams to quickly repair user impacting endpoint issues, reduce their overall risk posture, speed security threat response, and increase operations productivity. Ziften's secure enterprise architecture delivers continuous, streaming endpoint monitoring and historical data collection for large and mid-sized enterprises, governments, and managed security service providers (MSSP). And Ziften helps extend the value of incumbent tools, and fill the gaps between fragmented, siloed systems.

Fortinet and Ziften have partnered to deliver an industry-leading security solution that addresses these challenges. Ziften provides end-to-end visibility and analytics to provide security teams with endpoint context to rapidly detect, remediate, and respond to both known and unknown threats. Fortinet's award-winning FortiGate Enterprise Firewall Platform provides the industry's highest-performing firewall capabilities, and Fortinet's FortiGuard Security Subscription Services provide the industry's highest level of threat research, intelligence, and analytics. Bringing the Fortinet and Ziften products together into one integrated solution delivers comprehensive endpoint and network security protection.

Deployment Prerequisites

1. Fortinet FortiSandbox—Supported versions are 2.2.2 to 2.4.1
2. Ziften Zenith—Supported version is 5.0.11

For Ziften's license, please contact the appropriate channels through Ziften. To request an evaluation of Ziften's Zenith, contact support@ziften.com.

Note: Currently the FortiSandbox-Ziften integration does not support FortiSandbox Cloud deployments.

FORTINET
Fabric-Ready

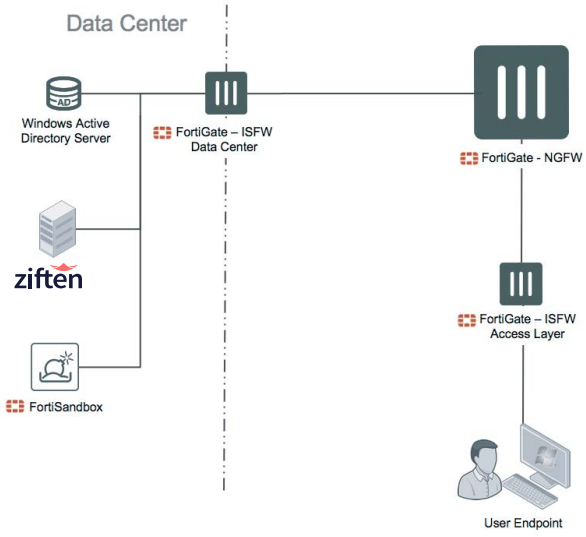

Figure 1: Topology.

Fortinet Configuration

1. Log in to the FortiSandbox.
2. Add a dedicated Administrator user for integrating with Ziften Zenith by navigating to System -> Administrators and selecting "+ Create New" at the top. See Figure 3.
3. Input the desired Administrator username and password, and make sure to enable "JSON API" at the bottom before creating this new user. See Figure 4.
4. Save the credentials for the user you just created, for inputting into the Ziften Zenith console to enable the integration.

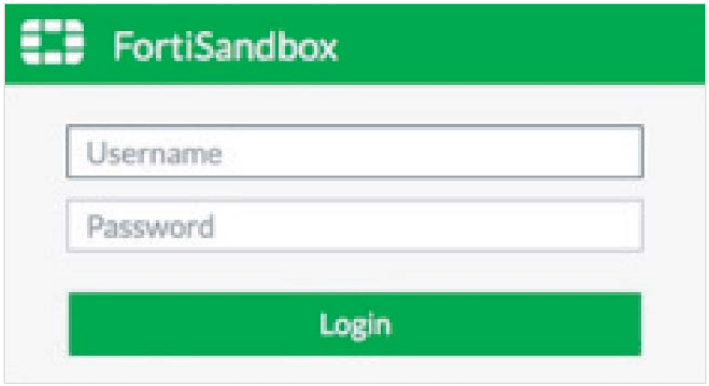

Figure 2: Log in to the FortiSandbox.

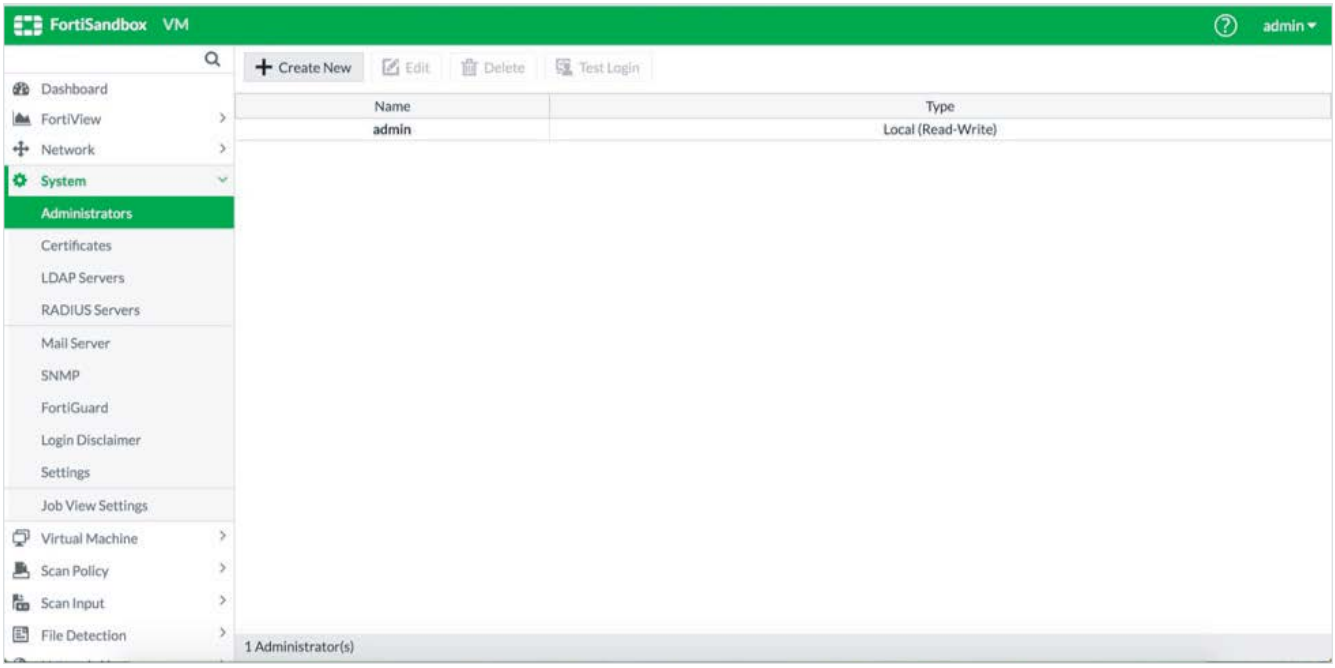

Figure 3: Add a dedicated administrator.

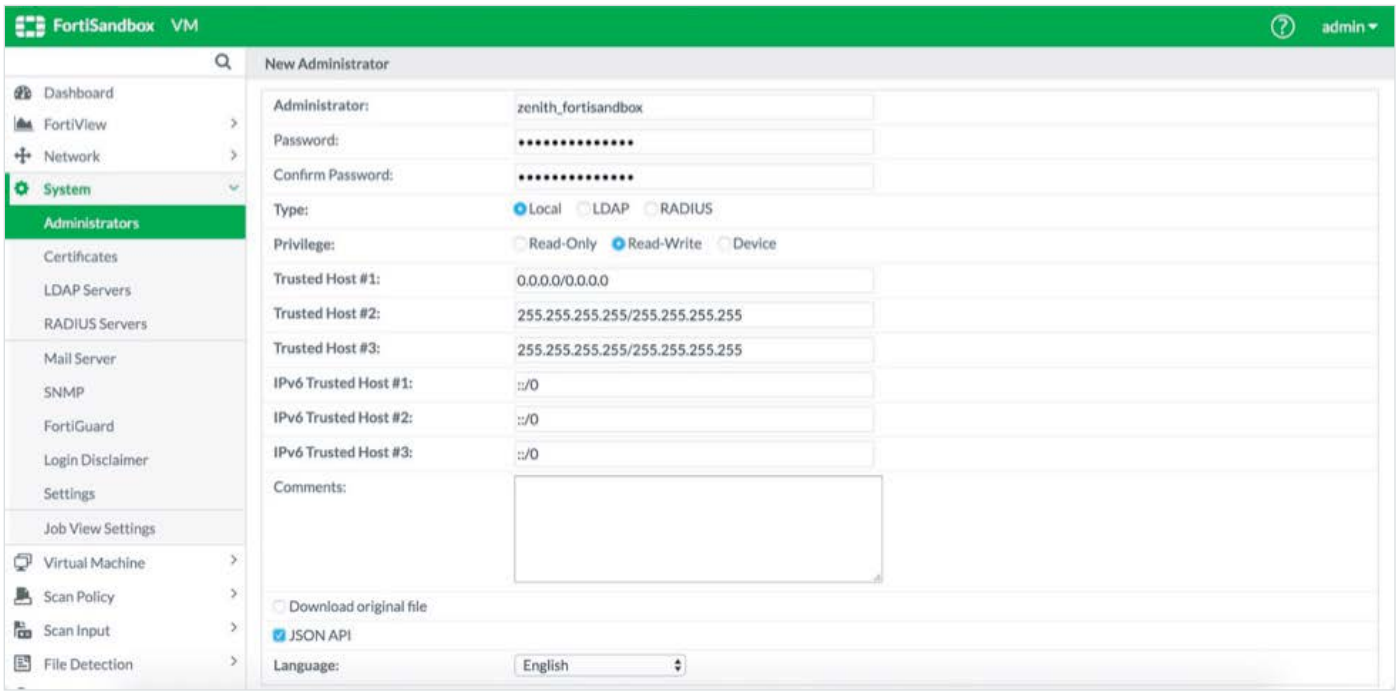

Figure 4: Input the desired administrator username and password.

Ziften Zenith Configuration

1. Log in to the Ziften Zenith console.
   Note: You will need to log in to Ziften using a user with Administrator privileges.
2. To enable the FortiSandbox integration, navigate to Admin -> Intelligence Sources. See Figure 6.
3. Click “ADD INTELLIGENCE SOURCE” at the top of the page, then select “FortiSandbox” from the drop-down menu. See Figure 7.
4. Fill in the “API base URL,” “Username,” and “Password” from your FortiSandbox environment, using the new credentials created in the FortiSandbox console. See Figure 8.
   - The format for the “API base URL” is https://[Hostname or IP]/jsonrpc (replace [Hostname or IP] with the appropriate details for your FortiSandbox deployment).
   - Make sure “Query for threat reports by binary’s hash” and “Submit files for analysis” are both enabled.
   - If desired, you can change the values for the “Throttle settings,” but the default values will work well for most environments.
   - You can select “TEST CONNECTION” to test the configuration with the URL and credentials you have typed in to ensure they are input properly.
5. Click “SAVE” to save the FortiSandbox settings. See Figure 9.
   - You can select “TEST CONNECTION” to test the configuration with the URL and credentials you have typed in to ensure they are input properly.

Figure 5: Log in to the Ziften Zenith Console.

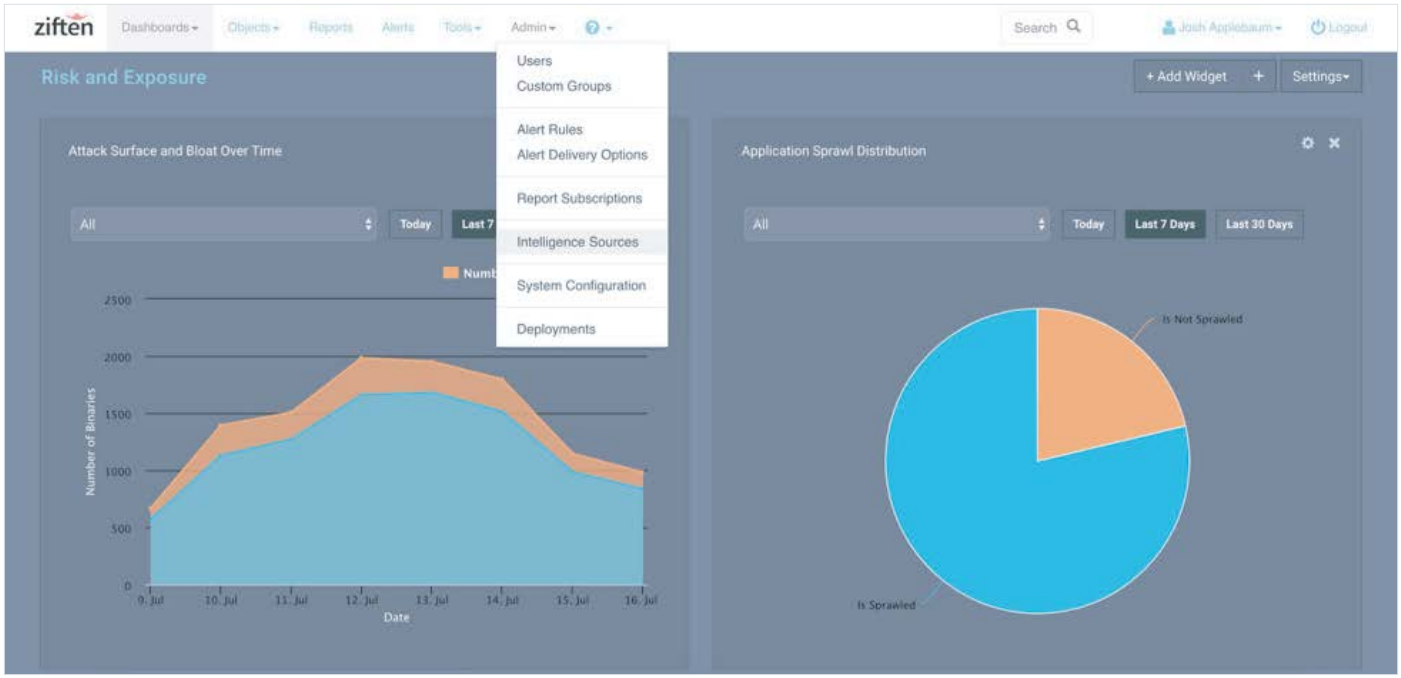

Figure 6: Enable the FortiSandbox Integration.

Figure 7: Add Intelligence Source.

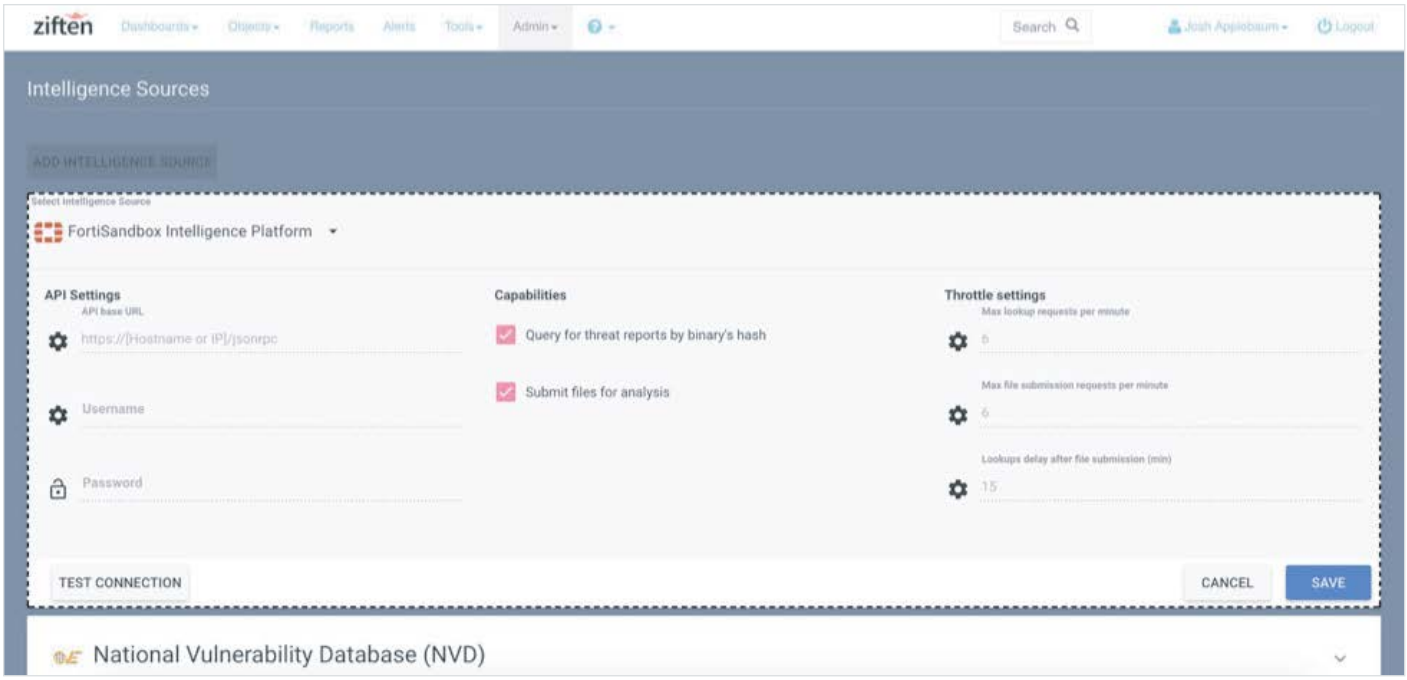

Figure 8: Fill in the API Base url, username, and password.

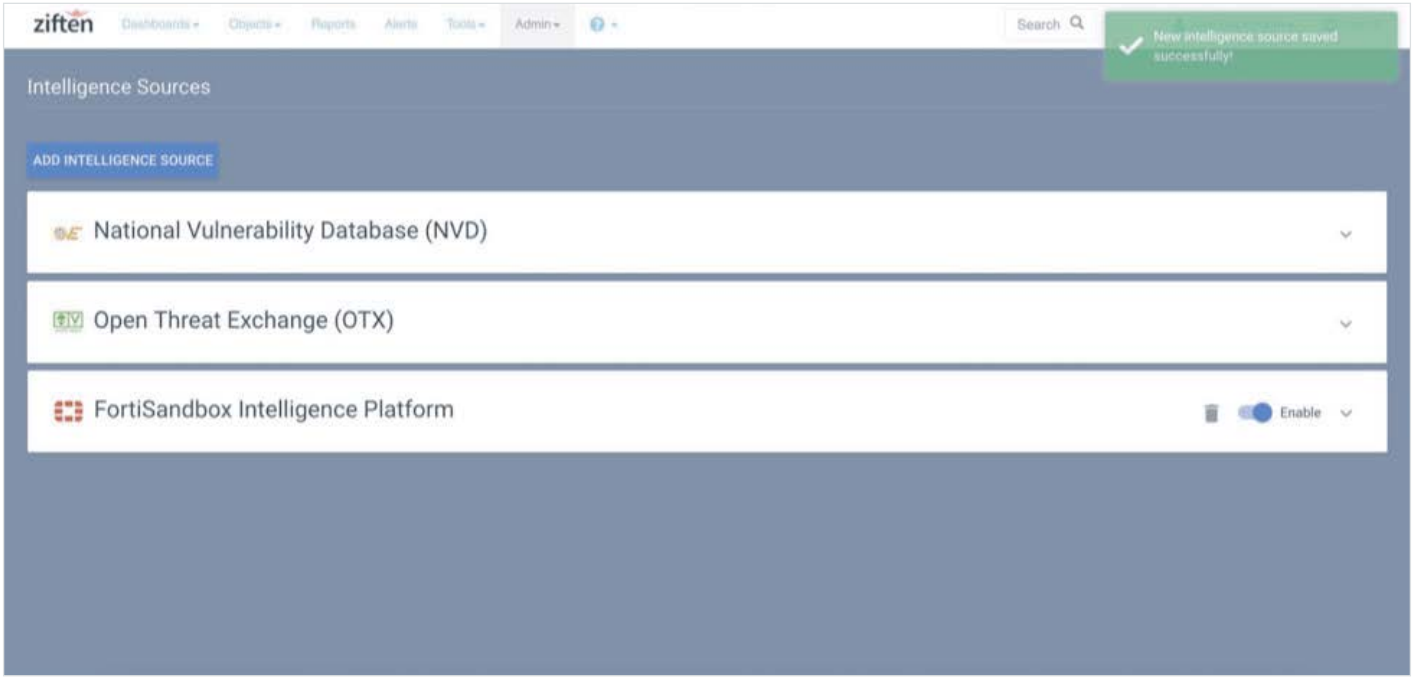

Figure 9: Click save.

Summary

- Access to FortiSandbox demo: https://fortisandbox.fortidemo.com.
- FortiSandbox Administration Guide: http://docs.fortinet.com/fortisandbox/admin-guides.
- FUSE: https://fuse.fortinet.com/p/fo/si/topic=47.
- Contact support@ziften.com (or your sales representative/sales engineer) if you need any assistance with the Ziften Zenith solution orfor any guides/documents.

July 17, 2019 4:07 AM

102032-A-A-EN

D:\Fortinet\Deployment Guide\Ziften Zenith\FA - DG - Ziften Zenith\FA - DG - Ziften Zenith