How-To Guide

Integrate Azure Front Door with Netsurion Open XDR

Publication Date

November 16, 2023

Abstract

This guide provides instructions to configure and integrate Azure Front Door with Netsurion Open XDR to retrieve its logs via Azure event hub and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Azure Front Door and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Azure Front Door in Netsurion Open XDR.

Table of Contents

1 Overview 4

2 Prerequisites 4

3 Integrating Azure Front Door with Netsurion Open XDR 4

3.1 Create Event Hub and Function App 4

3.2 Configuring Azure Front Door to Stream Events to Event Hub 4

4 Data Source Integration (DSI) in Netsurion Open XDR 6

4.1 Alerts 7

4.2 Reports 7

4.3 Dashboards 7

4.4 Saved Searches 7

1 Overview

Azure Front Door is Microsoft's modern cloud Content Delivery Network (CDN) that delivers fast, reliable, and secure global access to static and dynamic web content for users and applications.

Netsurion Open XDR manages logs retrieved from Azure Front Door through Azure Event hub.. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Azure Front Door.

2 Prerequisites

- An Azure subscription and a user who is a global administrator.
- An Azure Resource group.
- Netsurion Open XDR Manager details (Manager Hostname, Port, Manager public IP Address, and Organization name).
- The Data Source Integration package.

Note

To get the Data Source Integration package, contact your Netsurion Account Manager.

3 Integrating Azure Front Door with Netsurion Open XDR

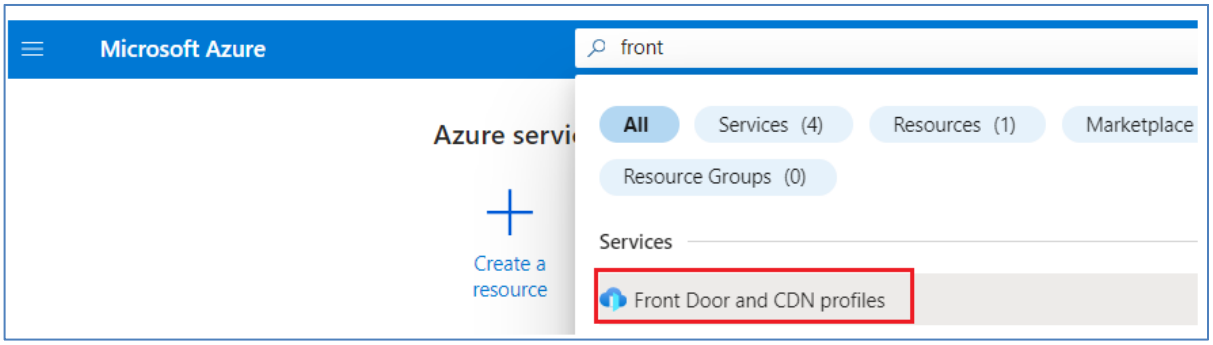
Azure Front Door can be integrated with Netsurion Open XDR by streaming the logs to Azure Event Hub, and from Azure Event Hub to Netsurion Open XDR using the Function App.

3.1 Create Event Hub and Function App

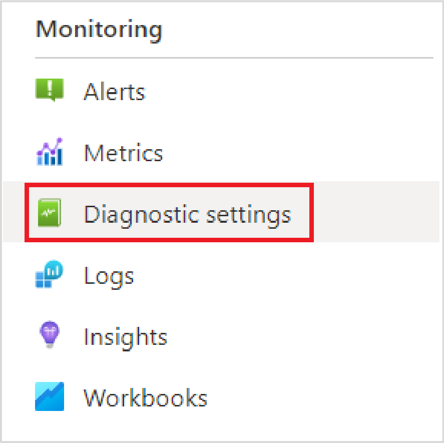
Refer to the configuration of Event Hub and Function App to forward the logs to Netsurion Open XDR.

3.2 Configuring Azure Front Door to Stream Events to Event Hub

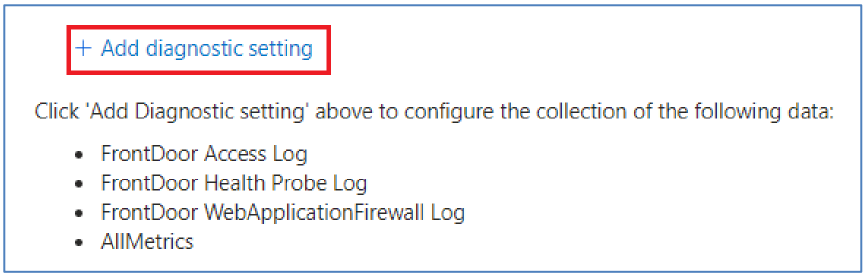
1. Login to portal.azure.com using the Azure admin account. Create and configure an event hub and function app, if not created.
2. Search and select **Front Door** from **All Services**.



3. Select the Front Door that needs to be monitored.
4. From the left panel under **Monitoring**, select **Diagnostic settings**.



5. Under **Diagnostic settings**, click **Add Diagnostic setting**.



Click 'Add Diagnostic setting' above to configure the collection of the following data:

- FrontDoor Access Log
- FrontDoor Health Probe Log
- FrontDoor WebApplicationFirewall Log
- AllMetrics

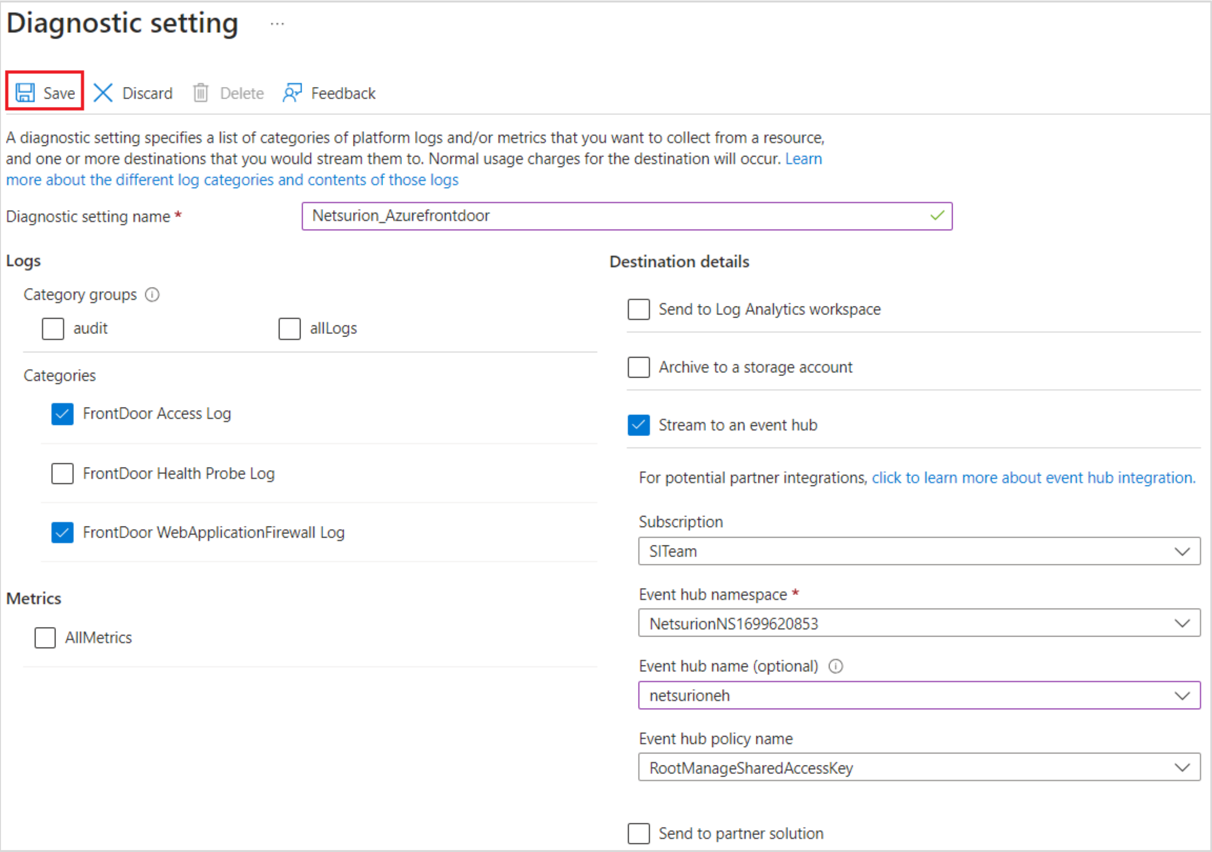
6. Provide the following details:

   Diagnostics Settings Name: **Netsurion_Azurefrontdoor**
   Select the below mentioned logs:

   - FrontDoor Access Log
   - FrontDoor WebApplicationFirewall Log

   In the **Destination details** section, select **Stream to an Event Hub** and then provide the following details:

   - **Subscription:** Select the desired Azure subscription.
   - **Event Hub namespace:** Select the Event Hub namespace.
   - **Event Hub name:** Select the Event Hub created under Event Hub namespace.
   - **Event Hub policy name:** Select the Event Hub policy (**RootManageSharedAccessKey**).



Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * Netsurion_Azurefrontdoor

Logs

Category groups

□ audit □ allLogs

Categories

☑ FrontDoor Access Log

□ FrontDoor Health Probe Log

☑ FrontDoor WebApplicationFirewall Log

Metrics

□ AllMetrics

Destination details

□ Send to Log Analytics workspace

□ Archive to a storage account

☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription: SITeam

Event hub namespace *: NetsurionNS1699620853

Event hub name (optional): netsurioneh

Event hub policy name: RootManageSharedAccessKey

□ Send to partner solution

7. Click **Save.**

4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following assets for **Azure Front Door**.

- Categories_Azure Front Door.iscat
- Alerts_Azure Front Door.isalt
- Reports_Azure Front Door.etcrx
- KO_Azure Front Door.etko
- Dashboards_Azure Front Door.etwd

Note

Refer the DSI Configuration guide for the procedures to configure the above DSI assets in Netsurion Open XDR.

The following are the key assets available in this Data Source Integration.

4.1 Alerts

Name	Description
Azure Front Door: Access control violation detected	Generated when an unauthorized/unauthenticated action is detected by Azure Front Door.
Azure Front Door: Potential threat detected	Generated when a potential threat event is detected by Azure Front Door.

4.2 Reports

Name	Description
Azure Front Door - WAF events	Provides details about the events that match a Web Application Firewall (WAF) rule in Azure Front Door
Azure Front Door - Audit events	Provides details about all the requests that go through Azure Front Door.

4.3 Dashboards

Name	Description
Azure Front Door - Geolocation of source IP address	Displays geolocation based on the source IP address of Azure Front Door access log.
Azure Front Door - Request overview	Displays Azure Front Door request based on HTTP requests.

4.4 Saved Searches

Name	Description
Azure Front Door - Audit events	Provides details about all the requests that go through the Azure Front Door.
Azure Front Door - WAF events	Provides details about the events that match a Web Application Firewall (WAF) rule in Azure Front Door.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support