How-To Guide

Integrate Proofpoint Email Protection with Netsurion Open XDR

Publication Date

Nov 24, 2023

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure and integrate Proofpoint Integrator with Netsurion Open XDR to retrieve its logs via API 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 Proofpoint and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Proofpoint in Netsurion Open XDR.

© Copyright Netsurion. All Rights Reserved.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

1 Overview

Proofpoint Email Protection provides multiple layers of security to protect from malware and non-malware threats, such as email fraud. It can manage all aspects of inbound and outbound emails to detect and block threats. It also prevents unauthorized access to confidential information.

Netsurion Open XDR manages logs retrieved from Proofpoint Email Protection. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Proofpoint Email Protection.

2 Prerequisites

- Netsurion XDR agent must be installed on the host system/ server.
- PowerShell 5.0 must be installed on the host system/ server.
- Users must have administrator privileges on the host system/ server to run PowerShell.
- Users must have root-level access to the Proofpoint console.
- The Data Source Integration package.

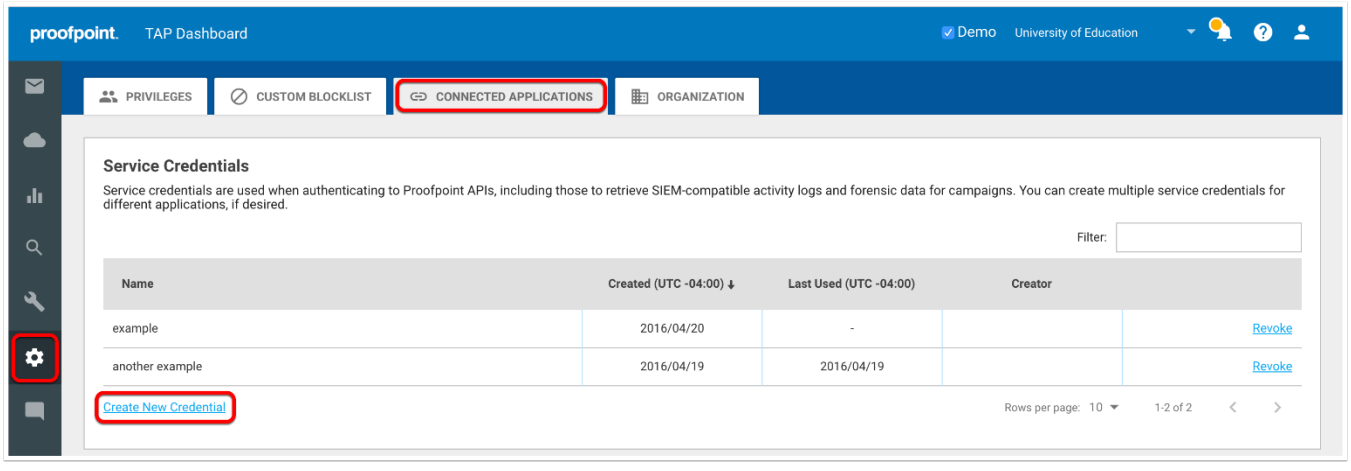
Note

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

3 Integrating Proofpoint with Netsurion Open XDR

3.1 Collecting Principal and Secret Key

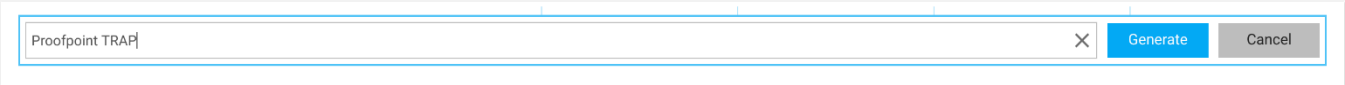
1. Login to the Proofpoint TAP dashboard account as an Administrator.
2. Navigate to **Settings** and then **Connected Applications**.



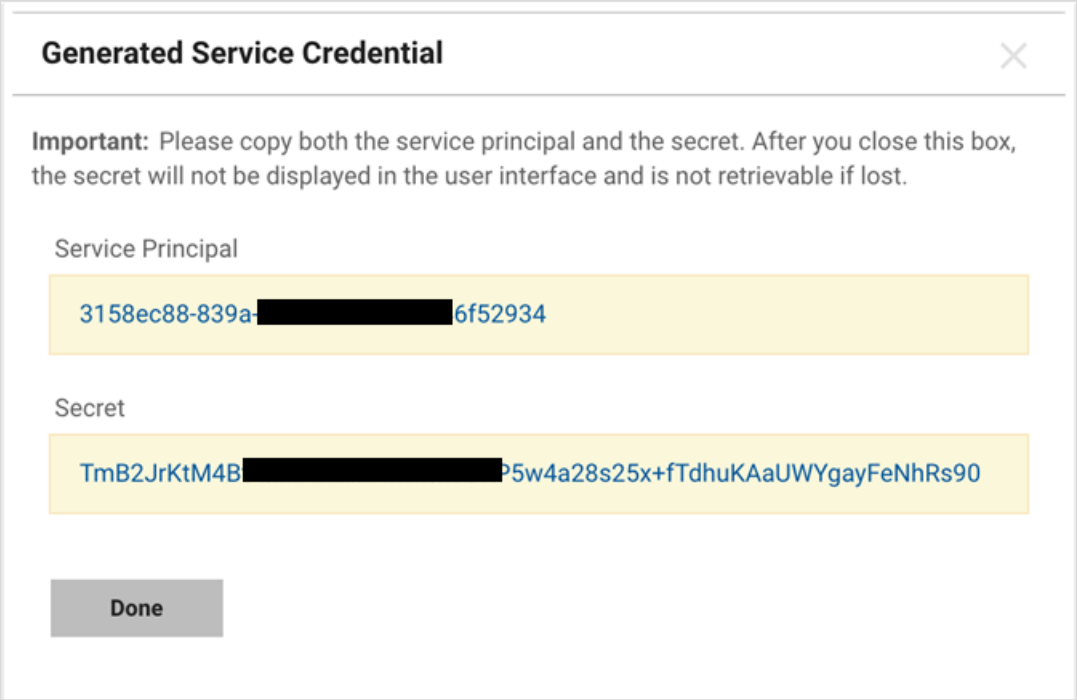
3. On the **Connected Applications** interface, click **Create New Credential**.

© Copyright Netsurion. All Rights Reserved.

4. Enter the name of the credential and click **Generate**.

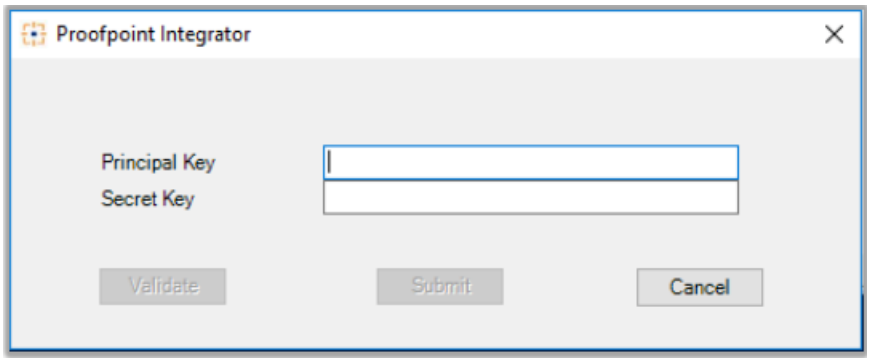


5. Copy the Service Principal and the Secret.



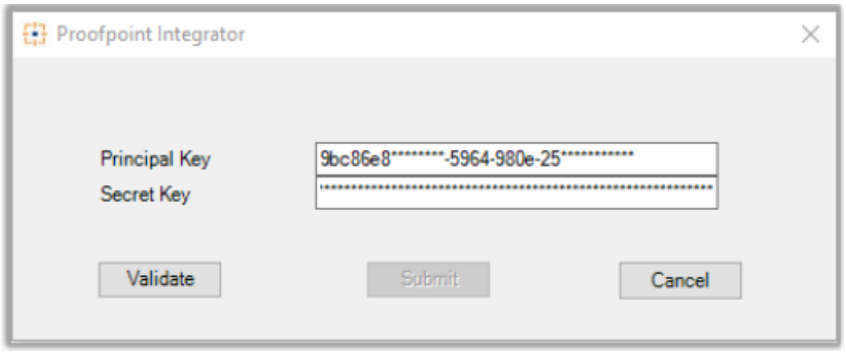
3.1.1 Forwarding Logs to Netsurion Open XDR

1. Contact the Netsurion Open XDR support team and get the **Proofpoint Integrator** executable file.
2. Right-click the file and select **Run as Administrator**.

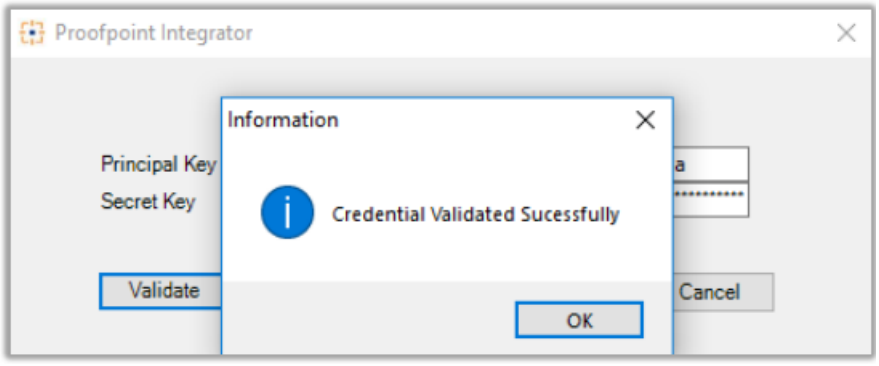


3. On the Proofpoint Integrator window, enter the **Principal Key** and the **Secret Key** obtained from the Proofpoint TAP dashboard.

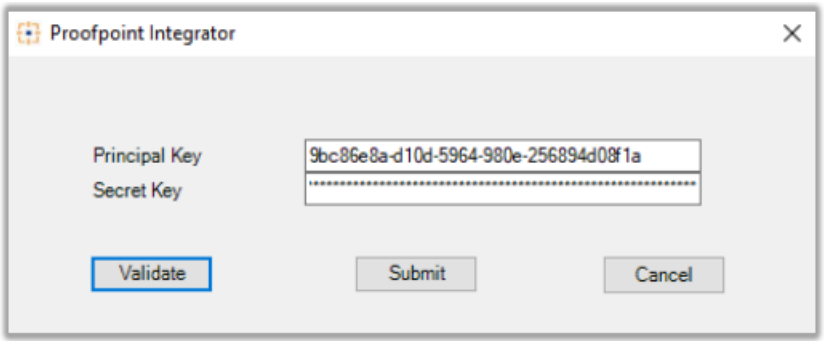
© Copyright Netsurion. All Rights Reserved.



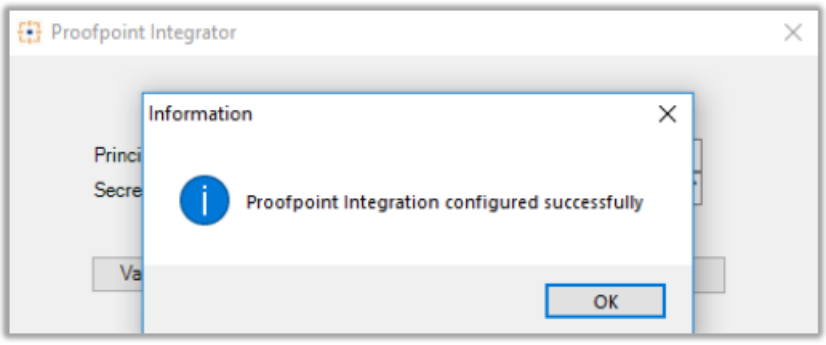
4. After entering the key details, click **Validate.** If the validation is successful, a success message will appear on the screen as shown below:



5. Click **OK** to close the Validation window. Finally, click the **Submit** button to complete the integration process.



6. Once the integration is successful, the success message appears as shown below:



© Copyright Netsurion. All Rights Reserved.

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 **Proofpoint**.

- Categories_Proofpoint.iscat
- Alerts_Proofpoint.isalt
- Flex_Reports_Proofpoint.etcrx
- KO_Proofpoint.etko
- Dashboard_Proofpoint.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
Proofpoint: Malware detected	Generated whenever malware is detected, and the malware status is active.

4.2 Reports

Name	Description
Proofpoint - Messages blocked	Provides details about the events that match a message blocked in Proofpoint.
Proofpoint - Messages delivered	Provides details about the events that match a message delivered in Proofpoint.
Proofpoint - Clicks permitted	Provides details about the events that match a permitted click in Proofpoint.
Proofpoint - Clicks blocked	Provides details about the events that match a blocked click in Proofpoint.

© Copyright Netsurion. All Rights Reserved.

4.3 Dashboards

Name	Description
Proofpoint - Blocked malicious attachments	Displays information about the malicious attachment names and the sender's email address.
Proofpoint - Blocked messages by IP address	Displays information about the sender's email address and the sender's IP address.

4.4 Saved Searches

Name	Description
Proofpoint - Clicks blocked	Provides details about the events that match a message blocked in Proofpoint.
Proofpoint - Clicks permitted	Provides details about the events that match a message delivered in Proofpoint.
Proofpoint - Messages blocked	Provides details about the events that match a permitted click in Proofpoint.
Proofpoint - Messages delivered	Provides details about the events that match a blocked click in Proofpoint.

© Copyright Netsurion. All Rights Reserved.

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

© Copyright Netsurion. All Rights Reserved.