



## Integration Guide

# Integrate Mimecast Secure Email Gateway with Netsurion Open XDR

### Publication Date

June 12, 2023

## Abstract

This guide provides instructions to configure and integrate Mimecast Secure Email Gateway with Netsurion Open XDR to retrieve its logs via syslog and forward it 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 Mimecast Secure Email Gateway and Netsurion Open XDR 9.3 or later.

## Audience

This guide is for the administrators responsible for configuring and monitoring Mimecast Secure Email Gateway in Netsurion Open XDR.

## Table of Contents

<b>1</b>	<b>Overview .....</b>	<b>4</b>
<b>2</b>	<b>Prerequisites .....</b>	<b>4</b>
<b>3</b>	<b>Integrating Mimecast Secure Email Gateway with Netsurion Open XDR .....</b>	<b>4</b>
3.1	Enable Logging for Your Account .....	4
3.2	Getting Authentication Token .....	5
3.2.1	Creating an API Key in Mimecast.....	5
3.2.2	Creating User Association Keys .....	7
3.2.3	Creating Python Script.....	8
3.3	Scheduling a Windows Task .....	9
<b>4</b>	<b>Data Source Integrations (DSIs) in Netsurion Open XDR .....</b>	<b>14</b>
4.1	Alerts .....	14
4.2	Reports .....	15
4.3	Dashboards .....	15
4.4	Saved Searches.....	15

## 1 Overview

Mimecast Secure Email Gateway is a cloud-based email management software. It helps stop email borne threats from attacking the networks and keeps sophisticated attackers out. It protects organizations and employees from spear-phishing, and provides anti-malware protection, anti-spam protection and zero-hour protection with multiple detection engines and intelligence feeds.

Netsurion Open XDR manages logs retrieved from Mimecast Secure Email Gateway. The alerts, reports, dashboard, and saved searches in Netsurion Open XDR are enhanced by capturing any suspicious activities.

## 2 Prerequisites

- **Mimecast Secure Email Gateway** latest version must be installed and configured.
- **Python 3.0 and above** must be installed.
- The Data Source Integration package.

### Note

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

## 3 Integrating Mimecast Secure Email Gateway with Netsurion Open XDR

### 3.1 Enable Logging for Your Account

1. Log in to the Mimecast Administration console and navigate to **Administration > Account > Account Settings**.
2. In **Account Settings**, go to the **Enhanced Logging** section and choose the required log type to enable.
  - a. **Inbound** - Logs for messages from external senders to internal recipients.
  - b. **Outbound** - Logs for messages from internal senders to external recipients.

### Note

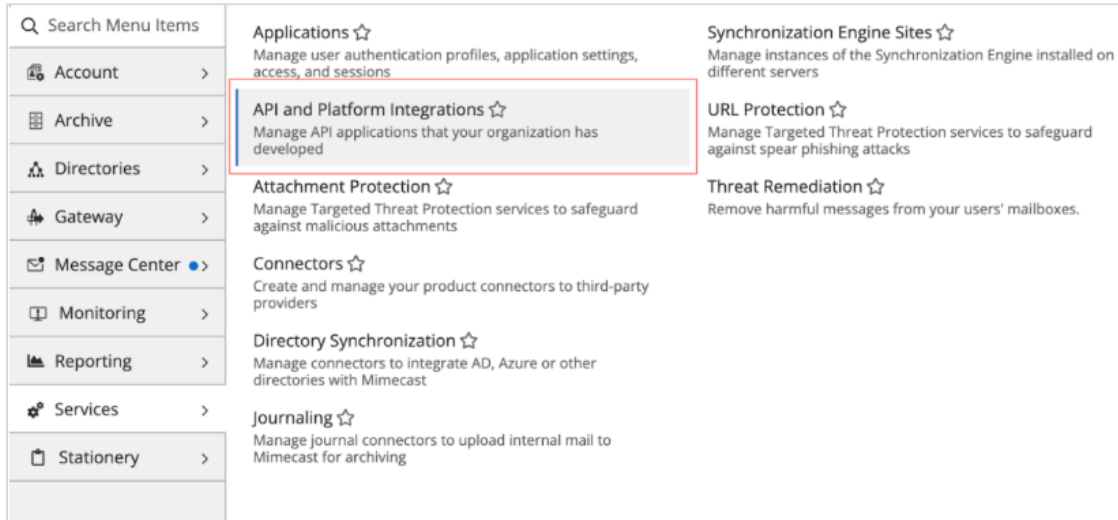
Do not select the Internal logs as it will increase the load on the Netsurion Open XDR receiver end.

3. After choosing the required log type, select **Save** to apply the changes.

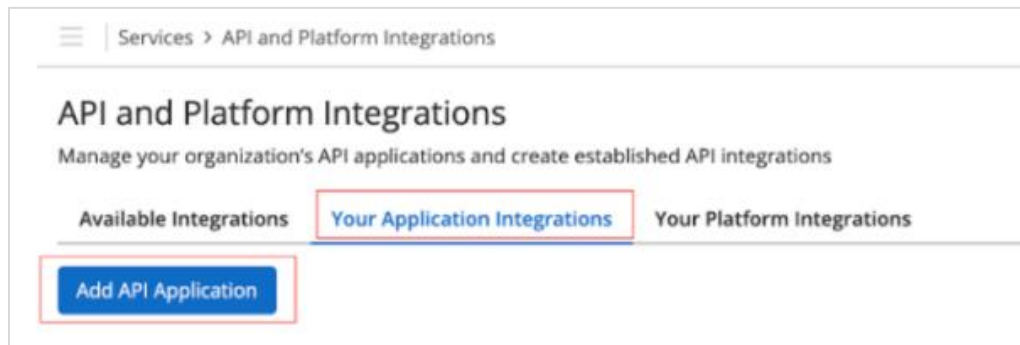
## 3.2 Getting Authentication Token

### 3.2.1 Creating an API Key in Mimecast

1. In the Mimecast Administration console, go to **Administration > Services > API and Platform Integrations**.



2. In the API and **Platform** Integrations interface, click **Add API Application** to create a new API application.



3. In the **Add API Application** interface, provide the following details.
  - a. Specify the **Application Name**.
  - b. Select the required **Category** from the drop-down list.
  - c. Select the **Enable Extended Session** check box for **Service Application**.
  - d. Specify the appropriate **Description**.

- e. Provide the **Developer** name and **Email** address.

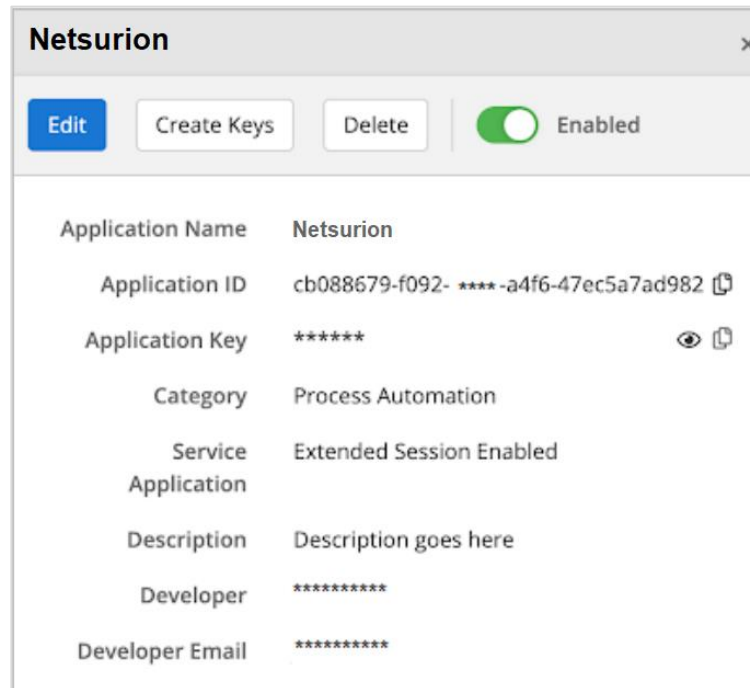
#### Note

For email address, it is advised to provide any service account.

4. After providing all the details, click **Next**.




5. In the **Summary** page, review to ensure all details are correct and click **Add**.

The application details are displayed on a slide panel.



**Netsurion** [X]

**Edit** **Create Keys** **Delete** ☒ **Enabled**

Application Name	Netsurion
Application ID	cb088679-f092- **** -a4f6-47ec5a7ad982 
Application Key	*****  
Category	Process Automation
Service Application	Extended Session Enabled
Description	Description goes here
Developer	*****
Developer Email	*****

6. Save the **Application ID** and **Application Key** for later use.

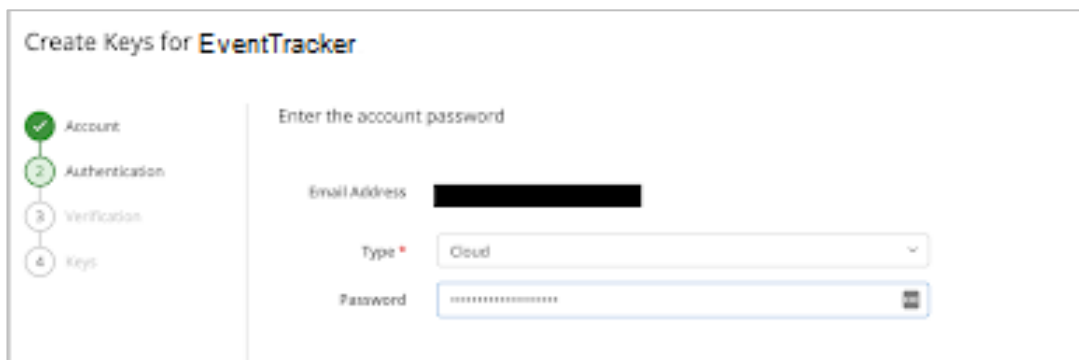
#### Note

Wait for 30 minutes before creating an API access and secret key.

### 3.2.2 Creating User Association Keys

After creating the application, create its user associated keys.

1. Go to **API Application** from the application list.
2. Click the **Create Keys** button, and the **Create Keys** wizard displays the selected Account tab.



Create Keys for **EventTracker**

☒ Account

☐ Authentication

☐ Verification

☐ Keys



Enter the account password

Email Address

Type

Password

Field / Option	Description
Email Address	Displays the service account email specified in the Account tab.
Type	Select the service account's password type (e.g., domain or cloud).
Password	Enter the service account's password.

3. Click **Next** to navigate to the Verification tab, and a verification code is sent by SMS.
4. Click **Next** to navigate to the Keys tab which displays the generated keys hidden by default.
  - Click the **View**  icon to display a key.
  - Click the **Copy**  icon to copy the key to the clipboard.
5. Copy and save the **accessKey** and **secretKey** values for later use.

### 3.2.3 Creating Python Script

1. Download the python script from [Mimecast](#) and save it with **.py** extension.
2. Open the python script in a python editor, such as IDLE and edit the **#Set up variables** section.

#### Note

Ensure whether the user running this script has the WRITE permission to the folder.

The following fields are required with adequate credentials as shown below.

#### IMPORTANT

The specified integration script details are provided by Mimecast. Netsurion do not have any permissions to modify the script. For any support, contact the Mimecast support team.

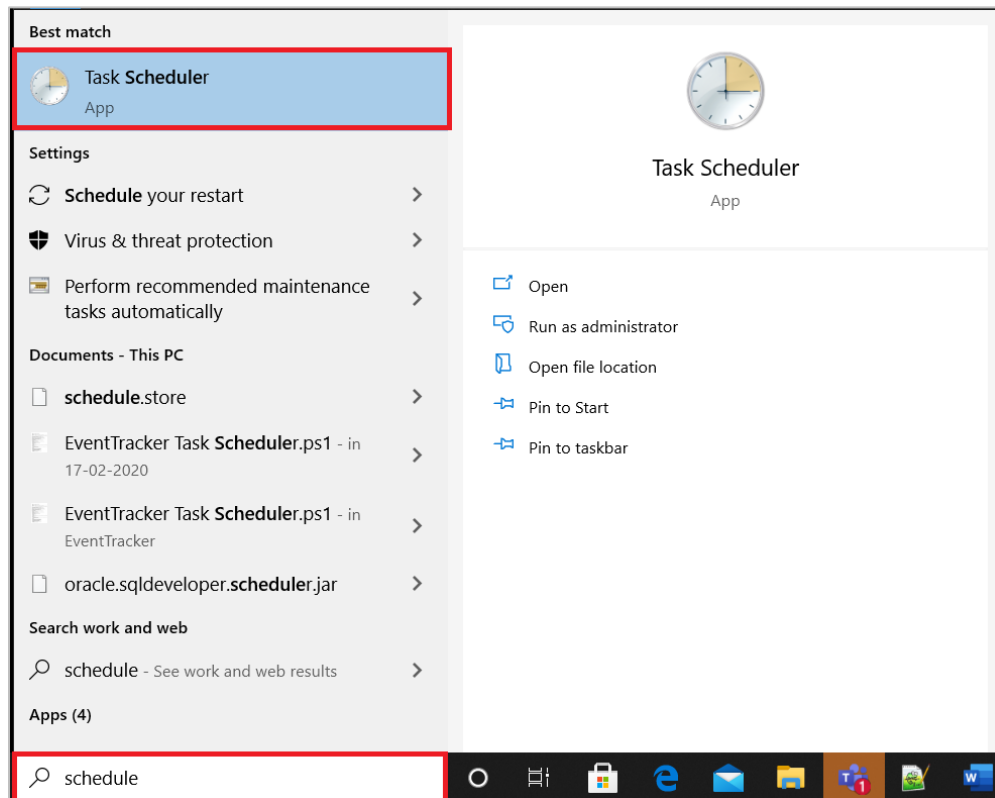
```
APP_ID = "YOUR DEVELOPER APPLICATION ID"
APP_KEY = "YOUR DEVELOPER APPLICATION KEY"
EMAIL_ADDRESS = 'EMAIL ADDRESS OF YOUR ADMINISTRATOR'
ACCESS_KEY = 'ACCESS KEY FOR YOUR ADMINISTRATOR'
SECRET_KEY = 'SECRET KEY FOR YOUR ADMINISTRATOR'
LOG_FILE_PATH = "FULLY QUALIFIED PATH TO FOLDER TO WRITE LOGS"
CHK_POINT_DIR = 'FULLY QUALIFIED PATH TO FOLDER TO WRITE PAGE TOKEN'
Syslog_Server = 'EventTracker Manager IP Address'
Syslog_port = 514
```

3. After providing the details, save and run the file. The script is ready to connect to Mimecast API.

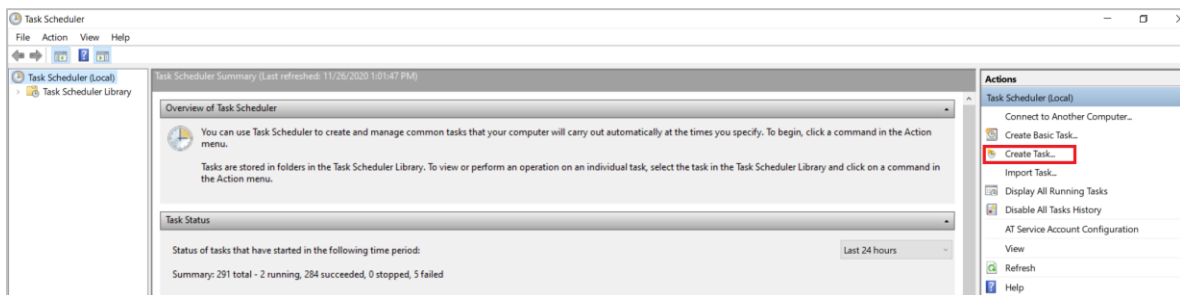


### 3.3 Scheduling a Windows Task

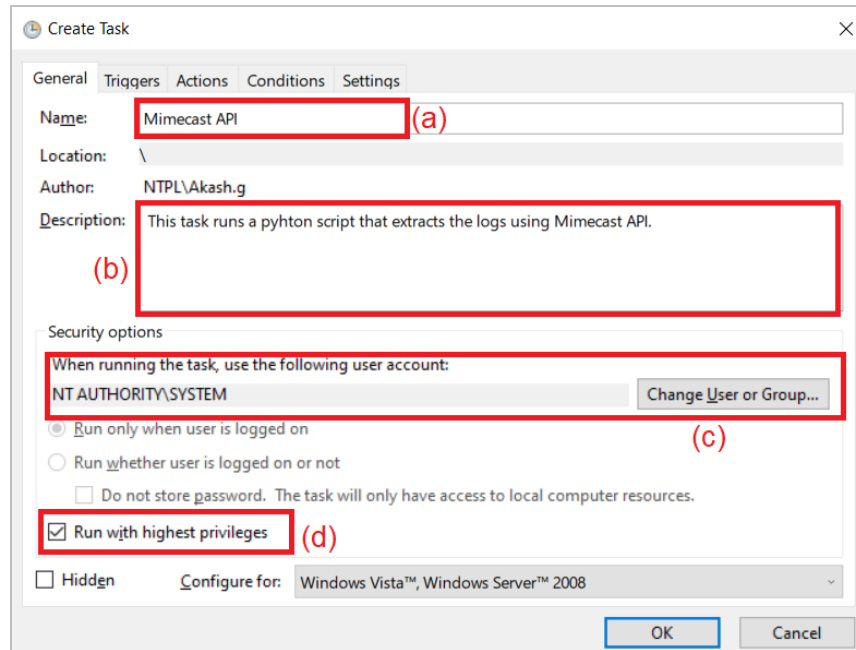
1. In the Windows taskbar, via the **Search** field type **Schedule** and choose **Task Scheduler**.



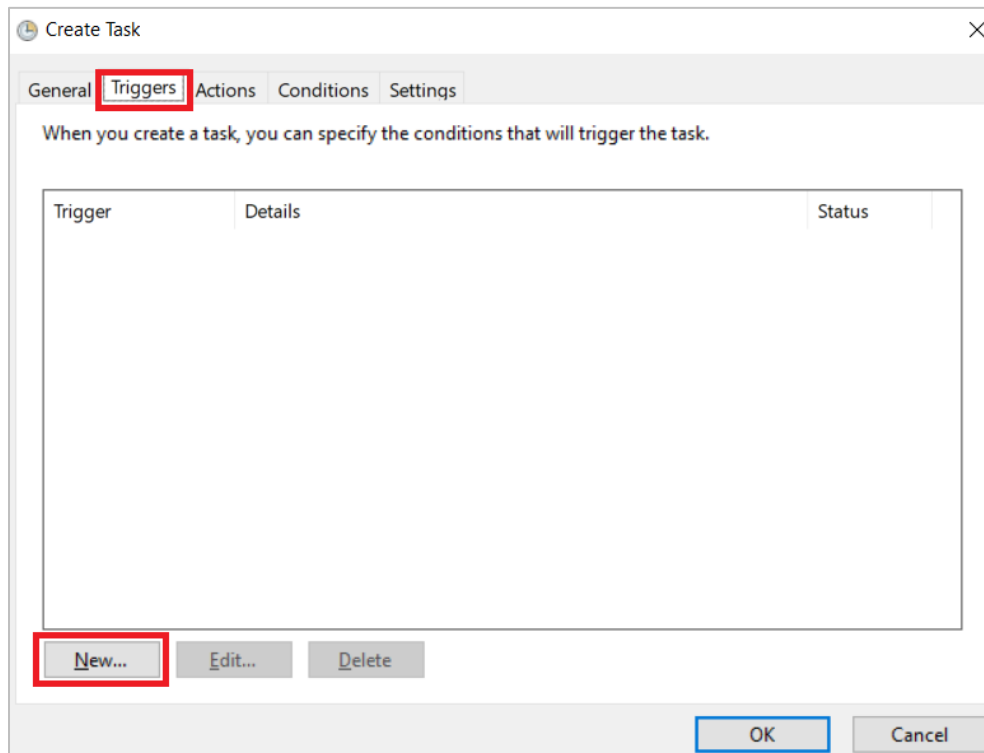
2. In the Task Scheduler window, click the **Create Task** link to open the wizard having the same name.



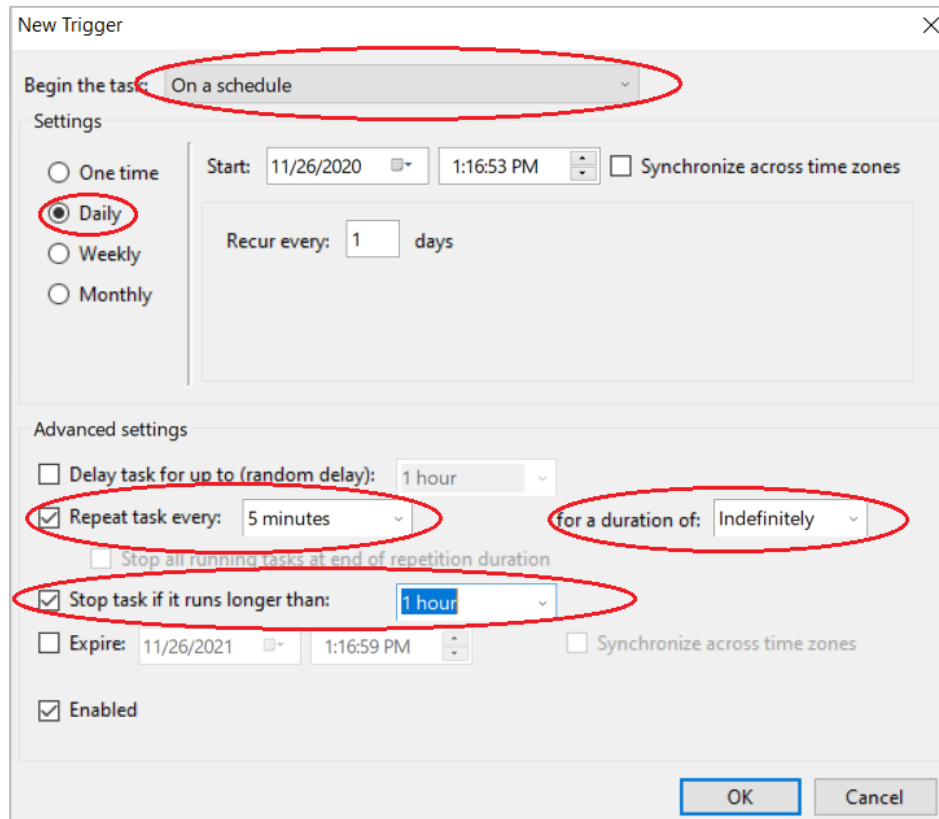
3. In the **Create Task** wizard > **General** tab, specify the following details.
  - a. **Name** to the task such as, **Mimecast API**.
  - b. **Description** of the task.
  - c. Click the **Change User or Group** button, to change the user account to **SYSTEM**.
  - d. Select the **Run with highest privileges** check box.



4. Next, go to the **Trigger** tab and click **New**.



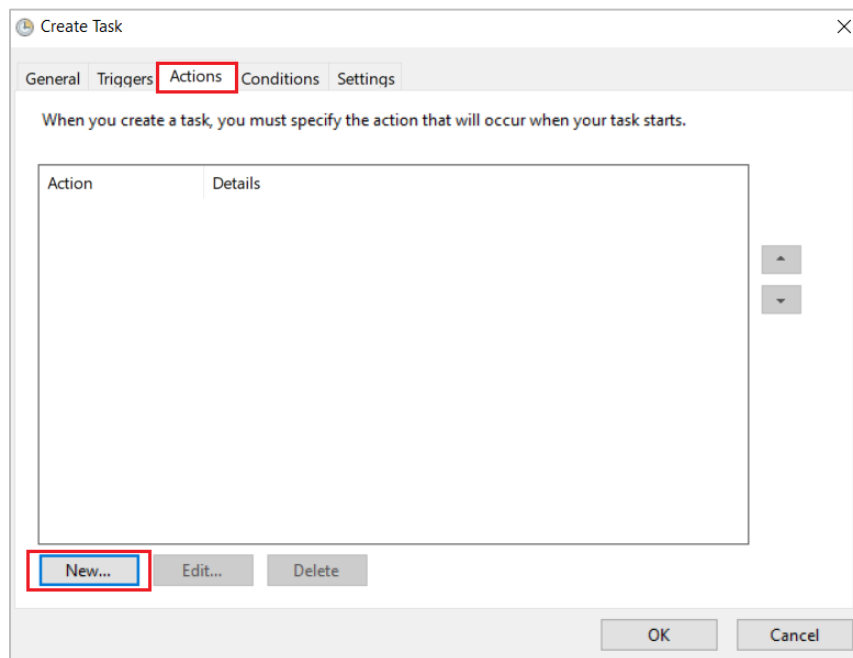
5. In the **New Trigger** window, configure the settings according to the following image and click **OK**.



The 'New Trigger' dialog box is configured as follows:

- Begin the task:** On a schedule
- Settings:**
  - One time:** ☐
  - Daily:** ☒ (circled in red)
  - Weekly:** ☐
  - Monthly:** ☐
- Start:** 11/26/2020 1:16:53 PM
- Synchronize across time zones:** ☐
- Recur every:** 1 days
- Advanced settings:**
  - Delay task for up to (random delay):** 1 hour
  - Repeat task every:** 5 minutes (circled in red)
  - for a duration of:** Indefinitely (circled in red)
  - Stop all running tasks at end of repetition duration:** ☐
  - Stop task if it runs longer than:** 1 hour (circled in red)
  - Expire:** 11/26/2021 1:16:59 PM
  - Synchronize across time zones:** ☐
  - Enabled:** ☒
- Buttons:** OK, Cancel

6. Then, go to the **Actions** tab and click **New**.



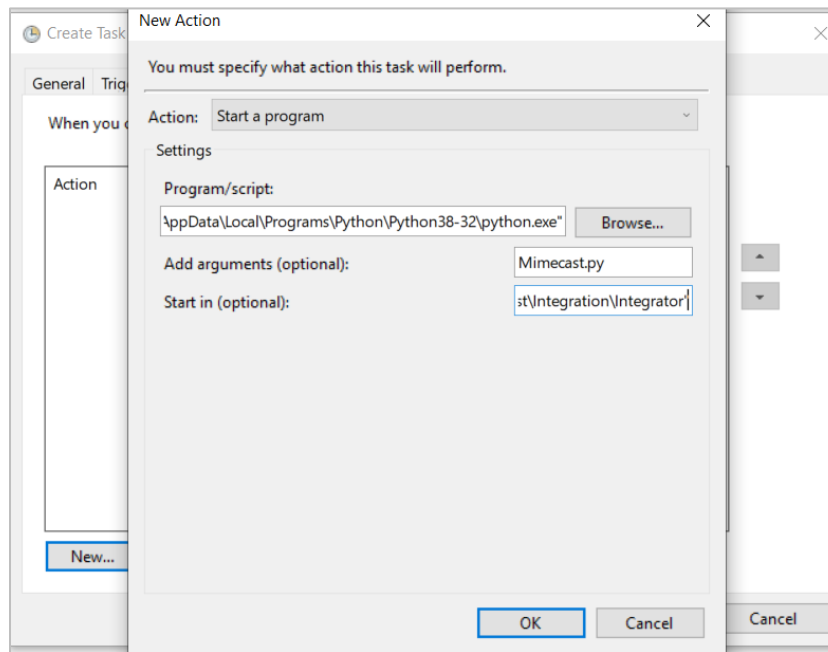
The 'Create Task' dialog box is configured as follows:

- Tabs:** General, Triggers, **Actions** (selected and circled in red), Conditions, Settings
- When you create a task, you must specify the action that will occur when your task starts.**
- Action/Details table:**

Action	Details
- Buttons:** New... (circled in red), Edit..., Delete
- Buttons:** OK, Cancel

7. In the **New Action** window > **Program/Script** field, click **Browse** to locate the Python Executable File  
For example, `C:\Users\user01\AppData\Local\Programs\Python\Python38-32\python.exe`.

8. In the **Add arguments (optional)** field, add the python file name, such as, **Mimecast.py**.
9. In the **Start in (optional)** box, add the python file location, such as, **D:\NetS\_Projects\Products\Mimecast\Integration\Integrator**.



Alternatively, you can also create a batch script and place it in the **Program/script**:

- a. Open a notepad and type in the specified configuration details and save the file as **MimecastPython.bat**.

*"Path where your Python exe is stored\python.exe" "Path where your Python script is stored\script name.py"*

For example,

```
"C:\Users\contoso\AppData\Local\Programs\Python\Python38-32\python.exe"
"D:\NetS_Projects\Products\Mimecast\Integration\Integrator\Mimecast.py"
```

- b. In the Task scheduler > **Action** tab, provide the batch file path.

For example, **D:\NetS\_Projects\Products\Mimecast\Integration\Integrator\MimecastPython.bat**.

10. After providing the details, click **OK**.

Edit Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script:  
cts\Mimecast\Integration\Integrator\MimecastPython.bat

Add arguments (optional):

Start in (optional):

OK Cancel

11. Click the **Settings** tab to ensure configuration matches as per the details highlighted in the following image, and then click **OK**.

Create Task

General Triggers Actions Conditions Settings

Specify additional settings that affect the behavior of the task.

☒ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☒ Stop the task if it runs longer than: 1 hour

☒ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

OK Cancel

## 4 Data Source Integrations (DSIs) 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 files for Mimecast Email Security Gateway.

- Categories\_Mimecast.iscat
- Alerts\_Mimecast.isalt
- Reports\_Mimecast.etcrx
- KO\_Mimecast.etko
- Dashboards\_Mimecast.etwd
- Filters\_Mimecast.isfil

### Note

Refer the [How To Configure DSI](#) guide for the procedures to configure the above DSIs in Netsurion Open XDR.

## Data Source Integrations Details

### 4.1 Alerts

Name	Description
Mimecast: Virus signature detection	Generated when a virus signature email is detected by Mimecast Secure Email Gateway.
Mimecast: Malicious file detected	Generated when an email containing malicious attachment is detected by Mimecast Secure Email Gateway.
Mimecast: Malicious URL detected	Generated when an email containing malicious URL is detected by Mimecast Secure Email Gateway.
Mimecast: Message has been quarantined	Generated when an email is held for review, and it is quarantined by Mimecast Secure Email Gateway.
Mimecast: Username has been impersonated	Generated when an email containing the spoofed internal user is detected by Mimecast Secure Email Gateway.

## 4.2 Reports

Name	Description
Mimecast - Inbound and outbound accepted emails	Provides details about all the inbound and outbound emails monitored by Mimecast Secure Email Gateway.
Mimecast - Rejected emails	Provides details about all the emails rejected by Mimecast Secure Email Gateway.
Mimecast - Spam emails	Provides details about all the spam emails detected by Mimecast Secure Email Gateway.
Mimecast - Virus signature detection	Provides details about all the emails containing virus signature or suspicious phishing detected by Mimecast Secure Email Gateway.

## 4.3 Dashboards

Name	Description
Mimecast - Rejected Emails by Sender	Displays all the rejected emails based on the sender email address.
Mimecast - Rejected Emails by Reason	Displays the reason of rejected emails captured by Mimecast secure email gateway.
Mimecast - Rejected Emails by Recipient	Displays the recipient of rejected emails captured by Mimecast secure email gateway.
Mimecast - Rejected Emails by Direction	Displays the direction of rejected emails captured by Mimecast secure email gateway.
Mimecast - Email Traffic by Status	Displays the status of the emails traffic captured by Mimecast Secure Email Gateway.
Mimecast - Email Traffic by Direction	Displays the direction of emails traffic captured by Mimecast Secure Email Gateway.
Mimecast - Email Traffic by Country	Displays the country details of emails traffic captured by Mimecast Secure Email Gateway.

## 4.4 Saved Searches

Name	Description
Mimecast - Inbound and outbound accepted emails	Provides details about all the inbound and outbound emails monitored by Mimecast Secure Email Gateway.
Mimecast - Rejected emails	Provides details about all the emails rejected by Mimecast Secure Email Gateway.
Mimecast - Spam emails	Provides details about all the spam emails detected by Mimecast Secure Email Gateway.
Mimecast - Virus signature detection	Provides details about all the emails containing virus signature or suspicious phishing detected by Mimecast Secure Email Gateway.

## 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](https://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	<a href="mailto:SOC@Netsurion.com">SOC@Netsurion.com</a>
Managed XDR Enterprise MSPs	<a href="mailto:SOC-MSP@Netsurion.com">SOC-MSP@Netsurion.com</a>
Managed XDR Essentials	<a href="mailto:Essentials-Support@Netsurion.com">Essentials-Support@Netsurion.com</a>
Software-Only Customers	<a href="mailto:Software-Support@Netsurion.com">Software-Support@Netsurion.com</a>

<https://www.netsurion.com/support>