

Administrator's Guide

Sumo Logic Data Collection Scripts for Mimecast allow a Mimecast administrator to download email, audit and SIEM events from Mimecast to be ingested by Sumo Logic or any platform thereafter. Data is pulled using Mimecast APIs, and then ingested by creating a Sumo Logic local file source or syslog source.

System Requirements and Prerequisites

Any available Server for Temporary Log Storage

Python v2.7.x installed on the server used to collect data from the Mimecast API

Network

Requires access to Mimecast API. Please ensure the server hosting the data collection scripts has outbound HTTPS access (TCP port 443) to the following hosts depending on the region where your Mimecast account is hosted:

Region	Host(s)
EU	api.mimecast.com AND eu-api.mimecast.com
US	api.mimecast.com AND us-api.mimecast.com
ZA	api.mimecast.com AND za-api.mimecast.com
AU	api.mimecast.com AND au-api.mimecast.com
Offshore	api.mimecast.com AND je-api.mimecast.com

Mimecast Permissions

The table below shows endpoints used by the collection scripts and the Mimecast administrator permissions required. For convenience all permissions are included in the Basic Administrator role.

Endpoint	Permission Required
----------	---------------------

/api/login/discover-authentication	n/a
/api/login/login	n/a
/api/audit/get-audit-events	Logs Read
/api/audit/get-siem-logs	Tracking Read

Preparation Steps

IMPORTANT: The data collection scripts require an Mimecast Administrator Authentication token.

By default an Authentication Tokens expire after **3 days**, this means that your scripts will **stop** collecting data from Mimecast after 3 days. For the best experience you **must** create a new user and Authentication Profile defining a longer lived Authentication Token. The steps below describe this process:

Step 1: Create a new user

- Login to the Administration Console.
- Navigate to the **Administration | Directories | Internal Directories** menu item to display a list of internal domains.
- Select the internal domain where you would like to create your new user.
- Select the **New Address** button from the menu bar.
- Complete the new address form and select **Save and Exit** to create the new user.
- Keep a note of the password set as you will use this when setting up the scripts.

Step 2: Add the user to an Administrative Role

- While logged into the Administration Console, navigate to the **Administration | Account | Roles** menu item to display the Roles page.
- Right click the **Basic Administrator** role and select **Add users to role**.
- Browse or search to find the new user created in the Step 1.
- Select the tick box to the left of the user.
- Select the **Add selected users** button to add the user to the role.

Step 3: Create a new group and add your new user

- While logged into the Administration Console, navigate to the **Administration | Directories | Profile Groups** menu item to display the Profile groups page.
- Create a new group by selecting the plus icon on the parent folder where you would like to create the group. This creates a new group with the Name "New Folder"
- To rename the group, select the newly created "New Folder" group. Then from the **Edit group** text box type the name you want to give the folder, for example Splunk Admin and press the Enter key to apply the change.
- With the group selected select the **Build** drop down button and select **Add Email Addresses**.
- Type the name of the new user created in Step 1.
- Select **Save and Exit** to add the new user to the group.

Step 4: Create a new Authentication Profile

- While logged into the Administration Console, navigate to the **Administration | Services | Applications** menu item to display the Application Settings page.
- Select the **Authentication Profiles** button.
- Select the **New Authentication Profile** button.
- Type a **Description** for the new profile.
- Set the **Authentication TTL** setting to **Never Expires**. This will make sure that when you create your Authentication Token it will not expire and impact the data collection of the app.
- Leave all other settings as their default.
- Select **Save and Exit** to create the profile.

Step 5: Create a new Application Setting

- While logged into the Administration Console, navigate to the **Administration | Services | Applications** menu item to display the Application Settings page.
- Select the **New Application Settings** button.
- Type a **Description**.
- Use the Group **Lookup** button to select the **Group** that you created in Step 3.
- Use the Authentication Profile **Lookup** button to select the **Authentication Profile** created in Step 4.
- Leave all other settings as their default.
- Select **Save and Exit** to create and apply the Application Settings to your new group and user.

Step 6: Enable logging for your account

- While logged into the Administration Console, navigate to the **Administration | Account | Account Settings** menu item to display the Account Settings page.

- Select the **Enhanced Logging** section.
- Select the types of logs you want to enable. The choices are:
 - Inbound - logs for messages from external senders to internal recipients
 - Outbound - logs for messages from internal senders to external recipients
 - Internal - logs for messages between internal domains
- Select **Save** to apply the changes.

Once these settings have been saved the Mimecast Mail Transfer Agent (MTA) will start logging data for your account and logs should start to become available for download up to 30 minutes after that.

You are now ready to set up the data collection scripts.

Set up Data Collection Scripts

Step 1: authentication_setup.py (Getting your authentication token)

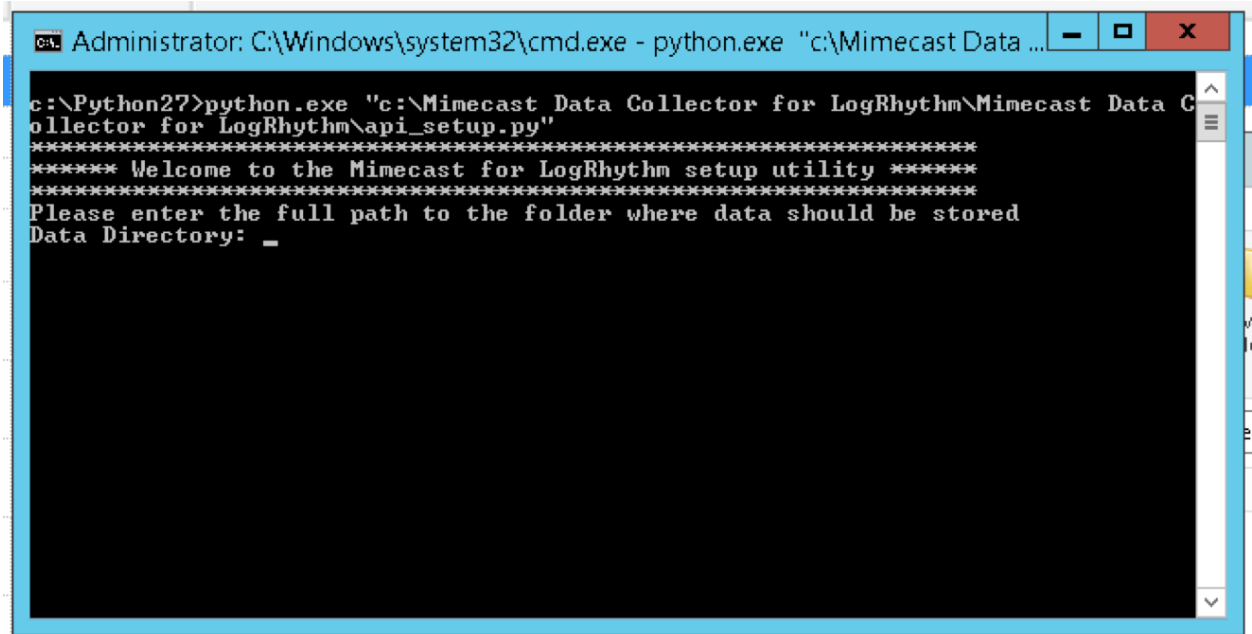
First, download and extract the data collection package from (*****here*****)

Mac OSX or *nix

- Open a terminal application.
- Navigate to the location where you extracted the package to.
- Execute the authentication_setup.py script to be guided through the steps required to request the required access key and secret key, like so:
- `python authentication_setup.py`
- This will create a config to be used later for log extraction.

Windows

- Open a Powershell window or command prompt.
- Change directory to the location where Python is installed like so:
- `cd C:\Python27`
- From here, execute the authentication_setup.py script as illustrated below, with:
 - `python.exe "<Path to data collection scripts>\authentication_setup.py"`



```
C:\Windows\system32\cmd.exe - python.exe "c:\Mimecast Data ...  
c:\Python27>python.exe "c:\Mimecast Data Collector for LogRhythm\Mimecast Data C  
ollector for LogRhythm\api_setup.py"  
***** Welcome to the Mimecast for LogRhythm setup utility *****  
*****  
Please enter the full path to the folder where data should be stored  
Data Directory: _
```

- This will create a config to be used later for log extraction.

MAC OSX, *nix, Windows

- When prompted enter the location where you would like to extract Mimecast data to. This will be a full path to the location on the server where Sumo Logic will later read and ingest logs from.
- Enter the email address of the administrator account created earlier in **Preparation Steps | Step 1: Set up your Mimecast administrator account**
- Enter the user's password
- You should see a message indicating the successful completion of the setup.
- Log in successful | Getting account code and saving config... | Config saved successfully.

Optional (necessary for continuous data collection)

IMPORTANT NOTE: Do not schedule log collection frequency for under 30 minutes. Logs are generated every 30 minutes from Mimecast.

MAC OSX, *nix

Use CRONTAB to define collection times and ranges: <https://www.howtogeek.com/101288/how-to-schedule-tasks-on-linux-an-introduction-to-crontab-files/>

- Set the schedule settings as desired. Recommendation: run data collection scripts daily, every 30 minutes for an indefinite time.

Windows

Create a Scheduled Task to execute data collection

- On the server hosting the scripts open the Windows Task Scheduler
- Create new task
- On the General tab
 - provide a name, for example, Mimecast Log Collection
 - select the option to “Run whether user is logged on or not”

The screenshot shows the 'Create Task' dialog box in Windows Task Scheduler. The 'General' tab is selected. The 'Name' field contains 'Mimecast MTA Log Collection'. The 'Location' field is empty. The 'Author' field contains 'QA-LR0\Administrator'. The 'Description' field is empty. Under 'Security options', the text 'When running the task, use the following user account:' is followed by 'QA-LR0\Administrator' and a 'Change User or Group...' button. The radio button 'Run whether user is logged on or not' is selected. Below it, the checkbox 'Do not store password. The task will only have access to local computer resources.' is unchecked. The checkbox 'Run with highest privileges' is also unchecked. At the bottom, the 'Hidden' checkbox is unchecked, and the 'Configure for:' dropdown menu is set to 'Windows Vista™, Windows Server™ 2008'. The 'OK' and 'Cancel' buttons are at the bottom right.

- On the Triggers tab
 - Click New
 - Set the schedule settings as desired. Recommendation: run data collection scripts daily, every 30 minutes for an indefinite time.

New Trigger [X]

Begin the task: On a schedule ▾

Settings

☐ One time
☒ Daily
☐ Weekly
☐ Monthly

Start: 14/03/2018 [calendar icon] 20:07:06 [time spinner] ☐ Synchronize across time zones

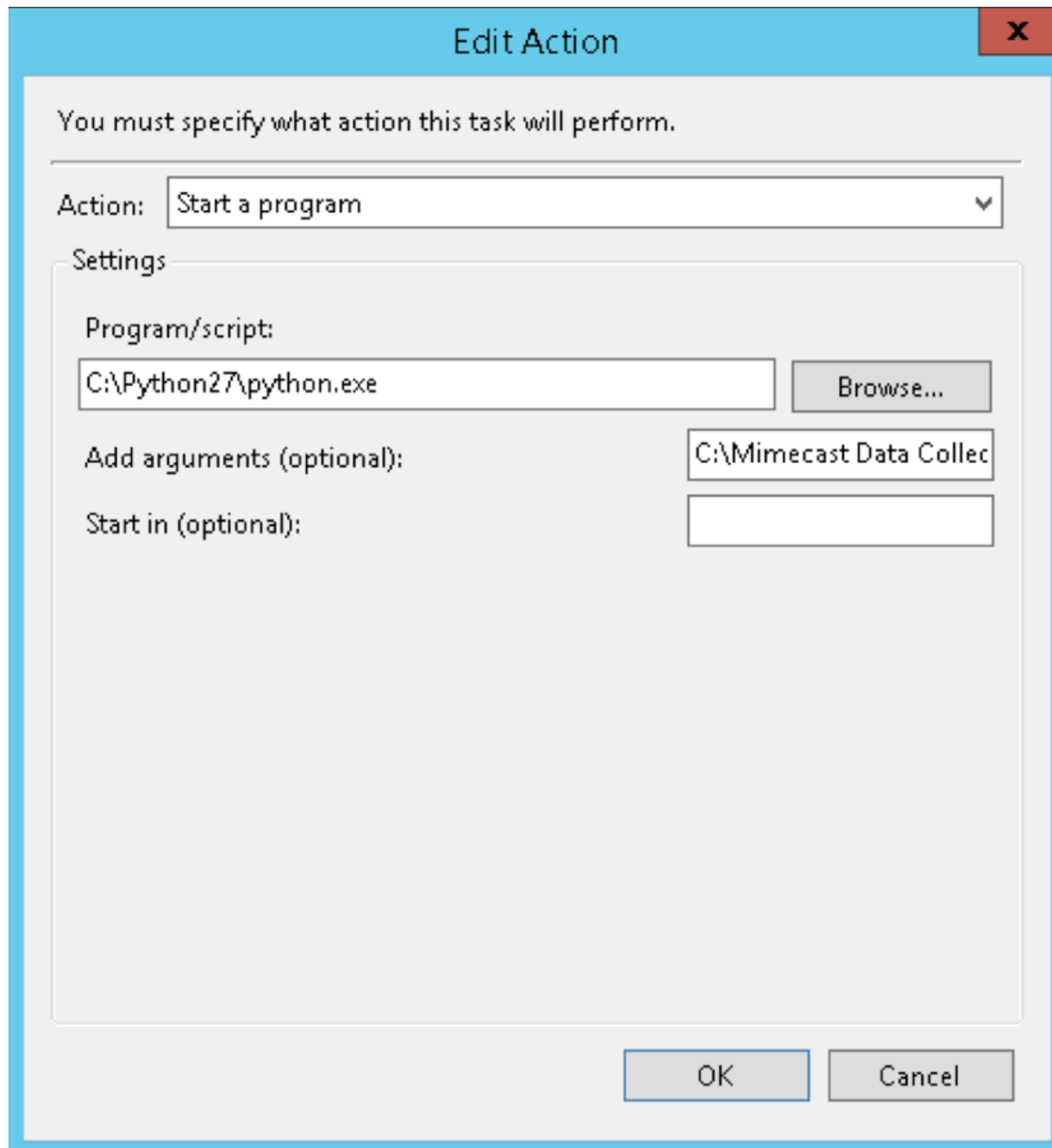
Recur every: 1 days

Advanced settings

☐ Delay task for up to (random delay): 1 hour ▾
☒ Repeat task every: 30 minutes ▾ for a duration of: Indefinitely ▾
☐ Stop all running tasks at end of repetition duration
☐ Stop task if it runs longer than: 3 days ▾
☐ Expire: 14/03/2019 [calendar icon] 20:07:06 [time spinner] ☐ Synchronize across time zones
☒ Enabled

OK Cancel

-
- Click OK
- On the Actions tab
 - Click New
 - Leave the Action as "Start a program"
 - In the Program / Script text box, enter the path to the python executable, for example, C:\Python27\python.exe
 - In the Add arguments / optional text box, enter the path to the script, for example,
C:\SumologicMimecast_Collection\DataCollectors\siem_collection.py



-
- Click OK.
- Configure any Conditions or Settings you want to apply. Click OK to save the task.
- Repeat this process for the audit_collection.py script.

Once complete the scripts will execute as scheduled or by selecting run now from the Task Scheduler and data should be downloaded to the data directory specified in setup.

NOTE: the data collection scripts will remove files not modified after 7 days to save disk space on the server.

Troubleshooting

The data collection scripts provided by Mimecast output a log file of activity for troubleshooting purposes. These logs are written to the logs directory in the location where the scripts are executed from, for example: C:\SumologicMimecast_Collection\log. Logs are kept for 7 days.

These logs (of logs) are used to diagnose issues when data is not being populated in the data directory. Mimecast/Sumo Logic support will require these logs to assist you with any issues.